

**Oracle® Communications  
Diameter Signaling Router**

Alarms and KPIs Reference

**E76928 Revision 01**

March 2017

## Oracle Communications Diameter Signaling Router Alarms and KPIs Reference

Copyright © 2011, 2016, 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.

# Table of Contents

|  |           |
|--|-----------|
| <b>Chapter 1: Introduction.....</b>                              | <b>27</b> |
| Revision History.....  | 28        |
| Overview.....  | 28        |
| Scope and Audience.....  | 28        |
| Manual Organization.....   | 28        |
| Documentation Admonishments.....                                 | 29        |
| Related Specifications.....                                      | 29        |
| Locate Product Documentation on the Oracle Help Center Site..... | 30        |
| Customer Training.....   | 30        |
| My Oracle Support (MOS).....                                     | 30        |
| Emergency Response.....  | 31        |
| <br>   |           |
| <b>Chapter 2: User Interface Introduction.....</b>               | <b>32</b> |
| User Interface Organization.....                                 | 33        |
| User Interface Elements.....                                     | 34        |
| Main Menu Options.....   | 35        |
| Missing Main Menu options.....                                   | 40        |
| Common Graphical User Interface Widgets.....                     | 40        |
| Supported Browsers.....  | 40        |
| System Login Page.....   | 40        |
| Main Menu Icons.....   | 42        |
| Work Area Displays.....  | 43        |
| Customizing the Splash Page Welcome Message.....                 | 46        |
| Column Headers (Sorting).....                                    | 46        |
| Page Controls.....   | 46        |
| Clear Field Control.....   | 47        |
| Optional Layout Element Toolbar.....                             | 47        |
| Filters.....   | 48        |
| Pause Updates.....   | 51        |
| Max Records Per Page Controls.....                               | 51        |
| <br>   |           |
| <b>Chapter 3: Alarms, Events, and KPIs Overview.....</b>         | <b>52</b> |
| Help Organization.....   | 53        |

|  |    |
|--|----|
| Alarms Warning.....                                      | 53 |
| General alarms and events information.....               | 53 |
| Alarms and events overview.....                          | 53 |
| Alarms formatting information.....                       | 55 |
| Alarm and event ID ranges.....                           | 55 |
| Alarm and event types.....                               | 56 |
| Viewing active alarms.....                               | 58 |
| Active alarms data export elements.....                  | 58 |
| Exporting active alarms.....                             | 59 |
| Generating a report of active alarms.....                | 60 |
| Viewing alarm and event history.....                     | 61 |
| Historical events data export elements.....              | 61 |
| Exporting alarm and event history.....                   | 62 |
| Generating a report of historical alarms and events..... | 63 |
| Viewing the file list.....                               | 63 |
| Opening a file.....                                      | 64 |
| Data Export.....   | 64 |
| Data Export elements.....                                | 64 |
| Configuring data export.....                             | 66 |
| Tasks.....   | 67 |
| Active Tasks.....  | 67 |
| Scheduled Tasks.....                                     | 70 |

## **Chapter 4: Alarms and Events.....73**

|   |    |
|---|----|
| IP Front End, IPFE (5000-5999).....                                   | 75 |
| 5001 - IPFE Backend Unavailable.....                                  | 75 |
| 5002 - IPFE address configuration error.....                          | 75 |
| 5003 - IPFE state sync run error.....                                 | 76 |
| 5004 - IPFE IP tables configuration error.....                        | 76 |
| 5005 - IPFE Backend In Stasis.....                                    | 77 |
| 5006 - Error reading from Ethernet device. Restart IPFE process. .... | 78 |
| 5007 - Out of Balance: Low.....                                       | 78 |
| 5008 - Out of Balance: High.....                                      | 78 |
| 5009 - No available servers in target set.....                        | 79 |
| 5010 - Unknown Linux iptables command error.....                      | 80 |
| 5011 - System or platform error prohibiting operation.....            | 80 |
| 5012 - Signaling interface heartbeat timeout.....                     | 81 |
| 5013 - Throttling traffic.....  | 81 |
| 5100 - Traffic overload.....  | 82 |
| 5101 - CPU Overload.....  | 82 |

|  |    |
|--|----|
| 5102 - Disk Becoming Full.....   | 83 |
| 5103 - Memory Overload.....  | 83 |
| OAM (10000-10999).....   | 83 |
| 10000 - Incompatible database version.....   | 83 |
| 10001 - Database backup started.....   | 84 |
| 10002 - Database backup completed.....   | 84 |
| 10003 - Database backup failed.....  | 84 |
| 10004 - Database restoration started.....  | 85 |
| 10005 - Database restoration completed.....  | 85 |
| 10006 - Database restoration failed.....   | 85 |
| 10008 - Database provisioning manually disabled .....  | 86 |
| 10009 - Config and Prov db not yet synchronized .....  | 86 |
| 10010 - Stateful db from mate not yet synchronized.....  | 86 |
| 10011 - Cannot monitor table.....  | 87 |
| 10012 - Table change responder failed .....  | 87 |
| 10013 - Application restart in progress .....  | 87 |
| 10020 - Backup failure .....   | 88 |
| 10050 - Resource Audit Failure.....  | 88 |
| 10051 - Route Deployment Failed.....   | 88 |
| 10052 - Route discovery failed.....  | 89 |
| 10053 - Route deployment failed - no available device.....                                       | 89 |
| 10054 - Device deployment failed.....  | 89 |
| 10055 - Device discovery failed.....   | 90 |
| 10073 - Server Group Max Allowed HA Role Warning.....  | 90 |
| 10074 - Standby server degraded while mate server stabilizes.....                                | 91 |
| 10075 - Application processes have been manually stopped.....                                    | 91 |
| 10078 - Application not restarted on standby server due to disabled failure cleanup<br>mode..... | 91 |
| 10100 - Log export started.....  | 92 |
| 10101 - Log export successful.....   | 92 |
| 10102 - Log export failed.....   | 93 |
| 10103 - Log export already in progress.....  | 93 |
| 10104 - Log export file transfer failed.....   | 93 |
| 10105 - Log export cancelled - user request.....   | 94 |
| 10106 - Log export cancelled - duplicate request.....  | 94 |
| 10107 - Log export cancelled - queue full.....   | 94 |
| 10108 - Duplicate scheduled log export task.....   | 95 |
| 10109 - Log export queue is full.....  | 95 |
| 10110 - Certificate About to Expire.....   | 96 |
| 10111 - Certificate Expired.....   | 96 |
| 10112 - Certificate Cannot Be Used.....  | 97 |

|   |     |
|---|-----|
| 10115 - Health Check Started.....                               | 97  |
| 10116 - Health Check Successful.....                            | 97  |
| 10117 - Health Check Failed.....                                | 98  |
| 10118 - Health Check Not Run.....                               | 98  |
| 10120 - Server Group Upgrade Started.....                       | 98  |
| 10121 - Server Group Upgrade Cancelled - Validation Failed..... | 99  |
| 10122 - Server Group Upgrade Successful.....                    | 99  |
| 10123 - Server Group Upgrade Failed.....                        | 99  |
| 10124 - Server Group Upgrade Cancelled - User Request.....      | 100 |
| 10130 - Server Upgrade Started.....                             | 100 |
| 10131 - Server Upgrade Cancelled.....                           | 100 |
| 10132 - Server Upgrade Successful.....                          | 101 |
| 10133 - Server Upgrade Failed.....                              | 101 |
| 10134 - Server Upgrade Failed.....                              | 101 |
| 10140 - Site Upgrade Started.....                               | 102 |
| 10141 - Site Upgrade Cancelled.....                             | 102 |
| 10142 - Site Upgrade Successful.....                            | 102 |
| 10143 - Site Upgrade Failed.....                                | 103 |
| 10144 - Site Upgrade Cancelled - User Request.....              | 103 |
| 10151 - Login successful.....                                   | 103 |
| 10152 - Login failed.....                                       | 104 |
| 10153 - Logout successful.....                                  | 104 |
| 10154 - User Account Disabled.....                              | 104 |
| 10155 - SAML Login Successful.....                              | 105 |
| 10156 - SAML Login Failed.....                                  | 105 |
| 10200 - Remote database reinitialization in progress.....       | 106 |
| 10300 - SNMP Trapping Not Configured.....                       | 106 |
| IDIH (11500-11549).....   | 106 |
| 11500 - Tracing Suspended.....                                  | 107 |
| 11501 - Trace Throttling Active.....                            | 107 |
| 11502 - Troubleshooting Trace Started.....                      | 107 |
| 11503 - Troubleshooting Trace Stopped.....                      | 108 |
| 11506 - Invalid IDIH-Trace AVP.....                             | 108 |
| 11507 - Unable to run network trace at this site.....           | 108 |
| 11508 - Network Trace Configuration Error.....                  | 109 |
| 11509 - Site Trace Configuration Error.....                     | 109 |
| 11510 - Network Trace Activation Error.....                     | 109 |
| 11511 - Invalid DIH HostName.....                               | 110 |
| SS7/Sigtran Alarms (19200-19299).....                           | 110 |
| 19200 - RSP/Destination unavailable.....                        | 110 |
| 19201 - RSP/Destination route unavailable.....                  | 111 |

|   |     |
|---|-----|
| 19202 - Linkset unavailable.....  | 111 |
| 19203 - Link unavailable.....   | 112 |
| 19204 - Preferred route unavailable.....  | 112 |
| 19205 - TFP received.....   | 113 |
| 19206 - TFA received.....   | 113 |
| 19207 - TFR received.....   | 114 |
| 19208 - TFC received.....   | 114 |
| 19209 - M3RL routing error.....   | 114 |
| 19210 - M3RL routing error - invalid NI.....  | 115 |
| 19211 - M3RL routing error - invalid SI.....  | 116 |
| 19217 - Node isolated - all links down.....   | 116 |
| 19226 - Timedout waiting for ASP-UP-ACK.....  | 117 |
| 19227 - Received unsolicited ASP-DOWN-ACK.....  | 117 |
| 19229 - Timed out waiting for ASP-ACTIVE-ACK.....   | 118 |
| 19230 - Received unsolicited ASP-INACTIVE-ACK.....  | 118 |
| 19231 - Received invalid M3UA message.....  | 119 |
| 19233 - Failed to send non-DATA message.....  | 119 |
| 19234 - Local link maintenance state change.....  | 120 |
| 19235 - Received M3UA error.....  | 120 |
| 19240 - Remote SCCP subsystem prohibited.....   | 121 |
| 19241 - SCCP malformed or unsupported message.....  | 122 |
| 19242 - SCCP Hop counter violation.....   | 123 |
| 19243 - SCCP routing failure.....   | 123 |
| 19244 - SCCP routing failure network status.....  | 124 |
| 19245 - SCCP GTT failure.....   | 124 |
| 19246 - Local SCCP subsystem prohibited.....  | 125 |
| 19248 - SCCP Segmentation Failure.....  | 125 |
| 19249 - SCCP Reassembly Failure.....  | 126 |
| 19250 - SS7 process CPU utilization.....  | 126 |
| 19251 - Ingress message rate.....   | 127 |
| 19252 - PDU buffer pool utilization.....  | 127 |
| 19253 - SCCP stack event queue utilization.....   | 128 |
| 19254 - M3RL stack event queue utilization.....   | 129 |
| 19255 - M3RL network management event queue utilization.....  | 129 |
| 19256 - M3UA stack event queue utilization.....   | 130 |
| 19258 - SCTP Aggregate Egress queue utilization.....  | 131 |
| 19259 - Operation discarded due to local resource limitation.....                                       | 131 |
| 19260 - Transaction could not be delivered to remote TCAP peer due to conditions<br>in the network..... | 132 |
| 19262 - Operation discarded due to malformed component received from remote<br>TCAP peer.....           | 132 |

|  |     |
|--|-----|
| 19263 - Transaction discarded due to malformed dialogue message received from local TC User..... | 133 |
| 19264 - Transaction discarded due to malformed dialogue message from remote TCAP peer.....       | 133 |
| 19265 - Unexpected event received from local TC User.....  | 133 |
| 19266 - Unexpected event received from remote TCAP peer.....                                     | 134 |
| 19267 - Dialogue removed by dialogue cleanup timer.....  | 134 |
| 19268 - Operation removed by invocation timer expiry.....  | 135 |
| 19269 - Dialogue aborted by remote TCAP peer.....  | 136 |
| 19270 - Received unsupported TCAP message.....   | 136 |
| 19271 - Operation rejected by remote TCAP peer.....  | 137 |
| 19272 - TCAP active dialogue utilization.....  | 137 |
| 19273 - TCAP active operation utilization.....   | 138 |
| 19274 - TCAP stack event queue utilization.....  | 138 |
| 19275 - Return error from remote TCAP peer.....  | 139 |
| 19276 - SCCP Egress Message Rate.....  | 139 |
| 19281 - TCAP Routing Failure.....  | 140 |
| Transport Manager Alarms and Events (19400-19419).....   | 140 |
| 19400 - Transport Down.....  | 140 |
| 19401 - Failed to configure Transport.....   | 141 |
| 19402 - Failed to connect Transport.....   | 142 |
| 19403 - Received malformed SCTP message (invalid length).....                                    | 142 |
| 19404 - Far-end closed the Transport.....  | 143 |
| 19405 - Transport closed due to lack of response.....  | 143 |
| 19406 - Local Transport maintenance state change.....  | 144 |
| 19407 - Failed to send Transport DATA Message.....   | 144 |
| 19408 - Single Transport Egress-Queue Utilization.....   | 145 |
| 19409 - Message Rejected by ACL Filtering.....   | 146 |
| 19410 - Adjacent Node IP Address state change.....   | 146 |
| 19411 - SCTP Transport closed due to failure of multihoming validation.....                      | 147 |
| 19412 - SCTP Transport configuration mismatched for Adjacent Node IP.....                        | 147 |
| 19413 - SCTP Transport closed due to unsupported peer address event recieved.....                | 147 |
| Communication Agent, ComAgent (19420-19909).....   | 148 |
| 19420 - BDFQFull.....  | 148 |
| 19421 - BDFThrotl.....   | 148 |
| 19422 - BDFInvalidPkt.....   | 149 |
| 19800 - Communication Agent Connection Down.....   | 149 |
| 19801 - Communication Agent Connection Locally Blocked.....                                      | 150 |
| 19802 - Communication Agent Connection Remotely Blocked.....                                     | 151 |
| 19803 - Communication Agent stack event queue utilization.....                                   | 152 |

|  |     |
|--|-----|
| 19804 - Communication Agent configured connection waiting for remote client to establish connection..... | 152 |
| 19805 - Communication Agent Failed To Align Connection.....  | 154 |
| 19806 - Communication Agent CommMessage mempool utilization.....   | 154 |
| 19807 - Communication Agent User Data FIFO Queue utilization.....  | 155 |
| 19808 - Communication Agent Connection FIFO Queue utilization.....                                       | 156 |
| 19810 - Communication Agent Egress Message Discarded.....  | 157 |
| 19811 - Communication Agent Ingress Message Discarded.....   | 157 |
| 19814 - Communication Agent Peer has not responded to heartbeat.....                                     | 158 |
| 19816 - Communication Agent Connection State Changed.....  | 158 |
| 19817 - Communication Agent DB Responder detected a change in configurable control option parameter..... | 159 |
| 19818 - Communication Agent DataEvent Mempool utilization.....   | 159 |
| 19820 - Communication Agent Routed Service Unavailable.....  | 160 |
| 19821 - Communication Agent Routed Service Degraded.....   | 160 |
| 19822 - Communication Agent Routed Service Congested.....  | 161 |
| 19823 - Communication Agent Routed Service Using Low-Priority Connection Group.....                      | 161 |
| 19824 - Communication Agent Pending Transaction Utilization.....   | 162 |
| 19825 - Communication Agent Transaction Failure Rate.....  | 163 |
| 19826 - Communication Agent Connection Congested.....  | 163 |
| 19827 - SMS stack event queue utilization.....   | 164 |
| 19830 - Communication Agent Service Registration State Change.....                                       | 164 |
| 19831 - Communication Agent Service Operational State Changed.....                                       | 165 |
| 19832 - Communication Agent Reliable Transaction Failed.....   | 165 |
| 19833 - Communication Agent Service Egress Message Discarded.....  | 166 |
| 19842 - Communication Agent Resource-Provider Registered.....  | 166 |
| 19843 - Communication Agent Resource-Provider Resource State Changed.....                                | 167 |
| 19844 - Communication Agent Resource-Provider Stale Status Received.....                                 | 167 |
| 19845 - Communication Agent Resource-Provider Deregistered.....  | 167 |
| 19846 - Communication Agent Resource Degraded.....   | 168 |
| 19847 - Communication Agent Resource Unavailable.....  | 168 |
| 19848 - Communication Agent Resource Error.....  | 169 |
| 19850 - Communication Agent Resource-User Registered.....  | 169 |
| 19851 - Communication Agent Resource-User Deregistered.....  | 169 |
| 19852 - Communication Agent Resource Routing State Changed.....  | 170 |
| 19853 - Communication Agent Resource Egress Message Discarded.....                                       | 170 |
| 19854 - Communication Agent Resource-Provider Tracking Table Audit Results.....                          | 171 |
| 19855 - Communication Agent Resource Has Multiple Actives.....   | 171 |
| 19856 - Communication Agent Service Provider Registration State Changed.....                             | 171 |
| 19857 - Communication Agent Service Provider Operational State Changed.....                              | 172 |

|   |     |
|---|-----|
| 19858 - Communication Agent Connection Rejected.....                                  | 172 |
| 19860 - Communication Agent Configuration Daemon Table Monitoring Failure.....        | 173 |
| 19861 - Communication Agent Configuration Daemon Script Failure.....                  | 173 |
| 19862 - Communication Agent Ingress Stack Event Rate.....                             | 174 |
| 19863 - Communication Agent Max Connections Limit In Connection Group<br>Reached..... | 174 |
| 19864 - ComAgent Successfully Set Host Server Hardware Profile.....                   | 175 |
| 19865 - ComAgent Failed to Set Host Server Hardware Profile.....                      | 175 |
| 19866 - Communication Agent Peer Group Status Changed.....                            | 176 |
| 19867 - Communication Agent Peer Group Egress Message Discarded.....                  | 176 |
| 19868 - Communication Agent Connection Rejected - Incompatible Network.....           | 176 |
| 19900 - Process CPU Utilization.....  | 177 |
| 19901 - CFG-DB Validation Error.....  | 177 |
| 19902 - CFG-DB Update Failure.....  | 178 |
| 19903 - CFG-DB post-update Error.....   | 178 |
| 19904 - CFG-DB post-update Failure.....   | 179 |
| 19905 - Measurement Initialization Failure.....                                       | 179 |
| Diameter Signaling Router (DSR) Diagnostics (19910-19999).....                        | 180 |
| 19910 - Message Discarded at Test Connection.....                                     | 180 |
| 19911 - Test message discarded .....  | 180 |
| Diameter Alarms and Events (8000-8299, 22000-22350, 22900-22999, 25500-25899).....    | 181 |
| 8000 - MpEvFsmException.....  | 181 |
| 8001 - MpEvException.....   | 185 |
| 8002 - MpEvRxException.....   | 185 |
| 8003 - MpEvTxException.....   | 193 |
| 8004 - EvFsmAdState.....  | 196 |
| 8005 - EvFsmOpState.....  | 196 |
| 8006 - EvFsmException.....  | 197 |
| 8007 - EvException.....   | 203 |
| 8008 - EvRxException.....   | 203 |
| 8009 - EvTxException.....   | 208 |
| 8010 - MpIngressDrop.....   | 212 |
| 8011 - EcRate.....  | 213 |
| 8012 - MpRxNgnPsOfferedRate.....  | 213 |
| 8013 - MpNgnPsStateMismatch.....  | 213 |
| 8014 - MpNgnPsDrop.....   | 214 |
| 8015 - NgnPsMsgMisrouted.....   | 214 |
| 8100 - NormMsgMisrouted.....  | 215 |
| 8101 - DiagMsgMisrouted.....  | 215 |
| 8200 - MpRadiusMsgPoolCongested.....  | 215 |
| 8201 - RclRxTaskQueueCongested.....   | 216 |

|   |     |
|---|-----|
| 8202 - RclItrPoolCongested.....   | 216 |
| 8203 - RclRxTaskQueueCongested.....   | 217 |
| 8204 - RclEtrPoolCongested.....   | 217 |
| 8205 - RadiusXactionFail.....   | 218 |
| 8206 - MpRxRadiusAllLen.....  | 219 |
| 8207 - MpRadiusKeyError.....  | 219 |
| 22001 - Message Decoding Failure.....   | 219 |
| 22002 - Peer Routing Rules with Same Priority.....  | 220 |
| 22004 - Maximum pending transactions allowed exceeded.....  | 220 |
| 22005 - No peer routing rule found.....   | 221 |
| 22007 - Inconsistent Application ID Lists from a Peer.....  | 221 |
| 22008 - Orphan Answer Response Received.....  | 222 |
| 22009 - Application Routing Rules with Same Priority.....   | 222 |
| 22010 - Specified DAS Route List not provisioned.....   | 223 |
| 22012 - Specified MCCA not provisioned.....   | 223 |
| 22013 - DAS Peer Number of Retransmits Exceeded for Copy.....   | 224 |
| 22014 - No DAS Route List specified.....  | 224 |
| 22016 - Peer Node Alarm Aggregation Threshold.....  | 224 |
| 22017 - Route List Alarm Aggregation Threshold.....   | 225 |
| 22018 - Maintenance Leader HA Notification to go Active.....  | 226 |
| 22019 - Maintenance Leader HA Notification to go OOS.....   | 226 |
| 22020 - Copy Message size exceeded the system configured size limit.....                                    | 226 |
| 22021 - Debug Routing Info AVP Enabled .....  | 227 |
| 22022 - Forwarding Loop Detected.....   | 227 |
| 22051 - Peer Unavailable.....   | 228 |
| 22052 - Peer Degraded.....  | 228 |
| 22053 - Route List Unavailable.....   | 229 |
| 22054 - Route List Degraded.....  | 229 |
| 22055 - Non-Preferred Route Group in Use.....   | 230 |
| 22056 - Connection Admin State Inconsistency Exists.....  | 231 |
| 22057 - ETG Rate Limit Degraded.....  | 231 |
| 22058 - ETG Pending Transaction Limit Degraded.....   | 232 |
| 22059 - Egress Throttle Group Message Rate Congestion Level changed.....                                    | 232 |
| 22060 - Egress Throttle Group Pending Transaction Limit Congestion Level<br>changed.....                    | 233 |
| 22061 - Egress Throttle Group Monitoring stopped.....   | 234 |
| 22062 - Actual Host Name cannot be determined for Topology Hiding.....                                      | 234 |
| 22063 - Diameter Max Message Size Limit Exceeded.....   | 235 |
| 22064 - Upon receiving Redirect Host Notification the Request has not been<br>submitted for re-routing..... | 235 |

|   |     |
|---|-----|
| 22065 - Upon receiving Redirect Realm Notification the Request has not been submitted for re-routing..... | 235 |
| 22066 - ETG-ETL Scope Inconsistency.....  | 236 |
| 22067 - ETL-ETG Invalid Association.....  | 236 |
| 22068 - TtpEvDoicException.....   | 237 |
| 22069 - TtpEvDoicOlr.....   | 239 |
| 22070 - TtpEvDegraded.....  | 239 |
| 22071 - TtgEvLossChg.....   | 240 |
| 22072 - TTP Degraded.....   | 241 |
| 22073 - TTP Throttling Stopped.....   | 241 |
| 22074 - TTP Maximum Loss Percentage Threshold Exceeded.....   | 242 |
| 22075 - Message is not routed to Application.....   | 242 |
| 22077 - MpExcessiveRerouteRate.....   | 242 |
| 22078 - Loop or Maximum Depth Exceeded in ART or PRT Search.....  | 243 |
| 22101 - FsmOpStateUnavailable.....  | 244 |
| 22102 - FsmOpStateDegraded.....   | 244 |
| 22103 - SCTP Path Unavailable.....  | 245 |
| 22104 - SCTPPathMismatch.....   | 245 |
| 22200 - MpCpuCongested.....   | 246 |
| 22201 - MpRxAllRate.....  | 246 |
| 22202 - MpDiamMsgPoolCongested.....   | 247 |
| 22203 - PTR Buffer Pool Utilization.....  | 247 |
| 22204 - Request Message Queue Utilization.....  | 248 |
| 22205 - Answer Message Queue Utilization.....   | 249 |
| 22206 - Reroute Queue Utilization.....  | 249 |
| 22207 - DclTxTaskQueueCongested.....  | 250 |
| 22208 - DclTxConnQueueCongested.....  | 250 |
| 22209 - Message Copy Disabled.....  | 251 |
| 22214 - Message Copy Queue Utilization.....   | 251 |
| 22221 - Routing MPS Rate.....   | 252 |
| 22222 - Long Timeout PTR Buffer Pool Utilization.....   | 252 |
| 22223 - MpMemCongested.....   | 253 |
| 22224 - Average Hold Time Limit Exceeded.....   | 254 |
| 22225 - MpRxDiamAllLen.....   | 254 |
| 22328 - IcRate.....   | 254 |
| 22349 - IPFE Connection Alarm Aggregation Threshold.....  | 255 |
| 22350 - Fixed Connection Alarm Aggregation Threshold.....   | 256 |
| 22900 - DPI DB Table Monitoring Overrun.....  | 257 |
| 22901 - DPI DB Table Monitoring Error.....  | 257 |
| 22950 - Connection Status Inconsistency Exists.....   | 257 |
| 22960 - DA-MP Profile Not Assigned.....   | 258 |

|  |     |
|--|-----|
| 22961 - Insufficient Memory for Feature Set.....   | 258 |
| 25607 - DSR Signaling Firewall is administratively Disabled.....                           | 259 |
| 25608 - Abnormal DA-MP Firewall.....   | 259 |
| 25609 - Firewall Configuration Error encountered.....                                      | 259 |
| 25610 - DSR Signaling Firewall configuration inconsistency detected.....                   | 260 |
| 25805 - Invalid Shared TTG Reference.....  | 260 |
| 25806 - Invalid Internal SOAM Server Group Designation.....                                | 261 |
| Range Based Address Resolution (RBAR) Alarms and Events (22400-22424).....                 | 261 |
| 22400 - Message Decoding Failure.....  | 261 |
| 22401 - Unknown Application ID.....  | 262 |
| 22402 - Unknown Command Code.....  | 262 |
| 22403 - No Routing Entity Address AVPs.....  | 263 |
| 22404 - No valid Routing Entity Addresses found.....                                       | 263 |
| 22405 - Valid address received didn't match a provisioned address or address<br>range..... | 263 |
| 22406 - Routing attempt failed due to internal resource exhaustion.....                    | 264 |
| 22407 - Routing attempt failed due to internal database inconsistency failure.....         | 264 |
| Generic Application Alarms and Events (22500-22599).....                                   | 265 |
| 22500 - DSR Application Unavailable.....   | 265 |
| 22501 - DSR Application Degraded.....  | 266 |
| 22502 - DSR Application Request Message Queue Utilization.....                             | 266 |
| 22503 - DSR Application Answer Message Queue Utilization.....                              | 267 |
| 22504 - DSR Application Ingress Message Rate.....  | 268 |
| 22520 - DSR Application Enabled.....   | 268 |
| 22521 - DSR Application Disabled.....  | 269 |
| Full Address Based Resolution (FABR) Alarms and Events (22600-22640).....                  | 269 |
| 22600 - Message Decoding Failure.....  | 269 |
| 22601 - Unknown Application ID.....  | 270 |
| 22602 - Unknown Command Code.....  | 270 |
| 22603 - No Routing Entity Address AVPs.....  | 271 |
| 22604 - No valid User Identity Addresses found .....                                       | 271 |
| 22605 - No Destination address is found to match the valid User Identity<br>address.....   | 271 |
| 22606 - Database or DB connection error.....   | 272 |
| 22607 - Routing attempt failed due to DRL queue exhaustion .....                           | 272 |
| 22608 - Database query could not be sent due to DB congestion.....                         | 273 |
| 22609 - Database connection exhausted.....   | 273 |
| 22610 - FABR DP Service congestion state change.....                                       | 274 |
| 22611 - FABR Blacklisted Subscriber.....   | 274 |
| 22631 - FABR DP Response Task Message Queue Utilization.....                               | 274 |
| 22632 - COM Agent Registration Failure.....  | 275 |

|  |     |
|--|-----|
| Policy and Charging Application (PCA) Alarms and Events (22700-22799).....             | 275 |
| 22700 - Protocol Error in Diameter Requests .....                                      | 275 |
| 22701 - Protocol Error in Diameter Answers.....  | 276 |
| 22702 - Database Hash Function Error.....  | 276 |
| 22703 - Diameter Message Routing Failure Due To Full DRL Queue.....                    | 276 |
| 22704 - Communication Agent Error.....   | 277 |
| 22705 - SBR Error Response Received.....   | 277 |
| 22706 - Binding Key Not Found In Diameter Message.....                                 | 278 |
| 22707 - Diameter Message Processing Failure.....                                       | 278 |
| 22708 - PCA Function is Disabled.....  | 278 |
| 22709 - PCA Function is Unavailable.....   | 279 |
| 22710 - SBR Sessions Threshold Exceeded.....   | 280 |
| 22711 - SBR Database Error.....  | 280 |
| 22712 - SBR Communication Error.....   | 281 |
| 22713 - SBR Alternate Key Creation Error.....  | 281 |
| 22714 - SBR RAR Initiation Error.....  | 281 |
| 22715 - SBR Audit Suspended.....   | 282 |
| 22716 - SBR Audit Statistics Report.....   | 282 |
| 22717 - SBR Alternate Key Creation Failure Rate.....                                   | 283 |
| 22718 - Binding Not Found for Binding Dependent Session Initiate Request.....          | 283 |
| 22719 - Maximum Number of Sessions per Binding Exceeded.....                           | 283 |
| 22720 - Policy SBR To PCA Response Queue Utilization Threshold Exceeded.....           | 284 |
| 22721 - Policy and Charging Server In Congestion.....                                  | 284 |
| 22722 - Policy Binding Sub-resource Unavailable.....                                   | 285 |
| 22723 - Policy and Charging Session Sub-resource Unavailable.....                      | 286 |
| 22724 - SBR Memory Utilization Threshold Exceeded.....                                 | 287 |
| 22725 - SBR Server In Congestion.....  | 287 |
| 22726 - SBR Queue Utilization Threshold Exceeded.....                                  | 288 |
| 22727 - SBR Initialization Failure.....  | 288 |
| 22728 - SBR Bindings Threshold Exceeded.....   | 289 |
| 22729 - PCRF Not Configured.....   | 289 |
| 22730 - Policy and Charging Configuration Error.....                                   | 289 |
| 22731 - Policy and Charging Database Inconsistency.....                                | 290 |
| 22732 - SBR Process CPU Utilization Threshold Exceeded.....                            | 291 |
| 22733 - SBR Failed to Free Binding Memory After PCRF Pooling Binding<br>Migration..... | 291 |
| 22734 - Policy and Charging Unexpected Stack Event Version.....                        | 292 |
| 22735 - Policy DRA session initiation request received with no APN.....                | 292 |
| 22736 - SBR failed to free shared memory after a PCA function is disabled.....         | 293 |
| 22737 - Configuration Database Not Synced.....   | 293 |
| 22738 - SBR Database Reconfiguration State Transition.....                             | 293 |

|  |     |
|--|-----|
| 22740 - SBR Reconfiguration Plan Completion Failure.....               | 294 |
| 22741 - Failed to route PCA generated RAR.....                         | 295 |
| 22750 - Enhanced Suspect Binding Removal Feature Enabled.....          | 295 |
| 22751 - Binding Audit Suppression by Suspect Binding Removal.....      | 295 |
| Tekelec Virtual Operating Environment, TVOE (24400-24499).....         | 296 |
| 24400 - TVOE libvirtd is down .....                                    | 296 |
| 24401 - TVOE libvirtd is hung .....                                    | 296 |
| 24402 - all TVOE libvirtd connections are in use .....                 | 297 |
| Computer Aided Policy Making, CAPM (25000-25499).....                  | 297 |
| 25000 - CAPM Update Failed.....  | 297 |
| 25001 - CAPM Action Failed.....  | 298 |
| 25002 - CAPM Exit Rule Template.....                                   | 298 |
| 25003 - CAPM Exit Trigger.....   | 299 |
| 25004 - Script failed to load.....                                     | 299 |
| 25005 - CAPM Generic Event.....  | 299 |
| 25006 - CAPM Generic Alarm - Minor.....                                | 300 |
| 25007 - CAPM Generic Alarm - Major.....                                | 300 |
| 25008 - CAPM Generic Alarm - Critical.....                             | 300 |
| OAM Alarm Management (25500-25899).....                                | 301 |
| 25500 - No DA-MP Leader Detected Alarm.....                            | 301 |
| 25510 - Multiple DA-MP Leader Detected Alarm.....                      | 301 |
| 25800 - Peer Discovery Failure.....                                    | 302 |
| 25801 - Peer Discovery Configuration Error Encountered.....            | 302 |
| 25802 - Realm Expiration Approaching.....                              | 302 |
| 25803 - Peer Discovery - Inconsistent Remote Host Port Assignment..... | 303 |
| 25804 - Peer Discovery State Change.....                               | 303 |
| Platform (31000-32800).....  | 304 |
| 31000 - S/W fault.....   | 304 |
| 31001 - S/W status.....  | 304 |
| 31002 - Process watchdog failure.....                                  | 305 |
| 31003 - Tab thread watchdog failure.....                               | 305 |
| 31100 - Database replication fault.....                                | 305 |
| 31101 - Database replication to slave failure.....                     | 306 |
| 31102 - Database replication from master failure.....                  | 306 |
| 31103 - DB Replication update fault.....                               | 306 |
| 31104 - DB Replication latency over threshold.....                     | 307 |
| 31105 - Database merge fault.....                                      | 307 |
| 31106 - Database merge to parent failure.....                          | 308 |
| 31107 - Database merge from child failure.....                         | 308 |
| 31108 - Database merge latency over threshold.....                     | 309 |
| 31109 - Topology config error.....                                     | 309 |

|   |     |
|---|-----|
| 31110 - Database audit fault.....                         | 309 |
| 31111 - Database merge audit in progress.....             | 310 |
| 31112 - DB replication update log transfer timed out..... | 310 |
| 31113 - DB replication manually disabled.....             | 311 |
| 31114 - DB replication over SOAP has failed.....          | 311 |
| 31115 - Database service fault.....                       | 311 |
| 31116 - Excessive shared memory.....                      | 312 |
| 31117 - Low disk free.....                                | 312 |
| 31118 - Database disk store fault.....                    | 313 |
| 31119 - Database updatelog overrun.....                   | 313 |
| 31120 - Database updatelog write fault.....               | 313 |
| 31121 - Low disk free early warning.....                  | 314 |
| 31122 - Excessive shared memory early warning.....        | 314 |
| 31123 - Database replication audit command complete.....  | 315 |
| 31124 - ADIC error.....                                   | 315 |
| 31125 - Database durability degraded.....                 | 315 |
| 31126 - Audit blocked.....                                | 316 |
| 31127 - DB Replication Audit Complete.....                | 316 |
| 31128 - ADIC Found Error.....                             | 316 |
| 31129 - ADIC Found Minor Issue.....                       | 317 |
| 31130 - Network health warning.....                       | 317 |
| 31131 - DB Ousted Throttle Behind.....                    | 318 |
| 31132 - DB Replication Precedence Relaxed.....            | 318 |
| 31133 - DB Replication Switchover Exceeds Threshold.....  | 318 |
| 31134 - DB Site Replication To Slave Failure.....         | 319 |
| 31135 - DB Site Replication From Master Failure.....      | 319 |
| 31136 - DB Site Replication Precedence Relaxed.....       | 320 |
| 31137 - DB Site Replication Latency Over Threshold.....   | 320 |
| 31140 - Database perl fault.....                          | 320 |
| 31145 - Database SQL fault.....                           | 321 |
| 31146 - DB mastership fault.....                          | 321 |
| 31147 - DB upsynclog overrun.....                         | 322 |
| 31148 - DB lock error detected.....                       | 322 |
| 31149 - DB Late Write Nonactive.....                      | 322 |
| 31200 - Process management fault.....                     | 323 |
| 31201 - Process not running.....                          | 323 |
| 31202 - Unkillable zombie process.....                    | 324 |
| 31206 - Process mgmt monitoring fault.....                | 324 |
| 31207 - Process resource monitoring fault.....            | 324 |
| 31208 - IP port server fault.....                         | 325 |
| 31209 - Hostname lookup failed.....                       | 325 |

|   |     |
|---|-----|
| 31213 - Process scheduler fault.....                | 326 |
| 31214 - Scheduled process fault.....                | 326 |
| 31215 - Process resources exceeded.....             | 326 |
| 31216 - SysMetric configuration error.....          | 327 |
| 31217 - Network Health Warning.....                 | 327 |
| 31220 - HA configuration monitor fault.....         | 328 |
| 31221 - HA alarm monitor fault.....                 | 328 |
| 31222 - HA not configured.....                      | 328 |
| 31223 - HA Heartbeat transmit failure.....          | 329 |
| 31224 - HA configuration error.....                 | 329 |
| 31225 - HA service start failure.....               | 329 |
| 31226 - HA availability status degraded.....        | 330 |
| 31227 - HA availability status failed.....          | 330 |
| 31228 - HA standby offline.....                     | 331 |
| 31229 - HA score changed.....                       | 331 |
| 31230 - Recent alarm processing fault.....          | 331 |
| 31231 - Platform alarm agent fault.....             | 332 |
| 31232 - Late heartbeat warning.....                 | 332 |
| 31233 - HA Path Down.....                           | 333 |
| 31234 - Untrusted Time Upon Initialization .....    | 333 |
| 31235 - Untrusted Time After Initialization .....   | 334 |
| 31236 - HA Link Down.....                           | 334 |
| 31240 - Measurements collection fault.....          | 334 |
| 31250 - RE port mapping fault.....                  | 335 |
| 31260 - SNMP Agent.....                             | 335 |
| 31261 - SNMP Configuration Error.....               | 336 |
| 31270 - Logging output.....                         | 336 |
| 31280 - HA Active to Standby transition.....        | 336 |
| 31281 - HA Standby to Active transition.....        | 337 |
| 31282 - HA Management Fault.....                    | 337 |
| 31283 - Lost Communication with server.....         | 338 |
| 31284 - HA Remote Subscriber Heartbeat Warning..... | 338 |
| 31285 - HA Node Join Recovery Entry.....            | 338 |
| 31286 - HA Node Join Recovery Plan.....             | 339 |
| 31287 - HA Node Join Recovery Complete.....         | 339 |
| 31288 - HA Site Configuration Error.....            | 340 |
| 31290 - HA Process Status.....                      | 340 |
| 31291 - HA Election Status.....                     | 340 |
| 31292 - HA Policy Status.....                       | 341 |
| 31293 - HA Resource Link Status.....                | 341 |
| 31294 - HA Resource Status.....                     | 341 |

|  |     |
|--|-----|
| 31295 - HA Action Status.....                        | 342 |
| 31296 - HA Monitor Status.....                       | 342 |
| 31297 - HA Resource Agent Info.....                  | 342 |
| 31298 - HA Resource Agent Detail.....                | 343 |
| 31299 - HA Notification Status.....                  | 343 |
| 31300 - HA Control Status.....                       | 343 |
| 31301 - HA Topology Events.....                      | 344 |
| 31322 - HA Configuration Error.....                  | 344 |
| 32100 - Breaker Panel Feed Unavailable.....          | 344 |
| 32101 - Breaker Panel Breaker Failure.....           | 345 |
| 32102 - Breaker Panel Monitoring Failure.....        | 345 |
| 32103 - Power Feed Unavailable.....                  | 345 |
| 32104 - Power Supply 1 Failure.....                  | 346 |
| 32105 - Power Supply 2 Failure.....                  | 346 |
| 32106 - Power Supply 3 Failure.....                  | 346 |
| 32107 - Raid Feed Unavailable.....                   | 347 |
| 32108 - Raid Power 1 Failure.....                    | 347 |
| 32109 - Raid Power 2 Failure.....                    | 347 |
| 32110 - Raid Power 3 Failure.....                    | 348 |
| 32111 - Device Failure.....                          | 348 |
| 32112 - Device Interface Failure.....                | 348 |
| 32113 - Uncorrectable ECC memory error.....          | 349 |
| 32114 - SNMP get failure.....                        | 349 |
| 32115 - TPD NTP Daemon Not Synchronized Failure..... | 350 |
| 32116 - TPD Server's Time Has Gone Backwards.....    | 350 |
| 32117 - TPD NTP Offset Check Failure.....            | 351 |
| 32300 - Server fan failure.....                      | 352 |
| 32301 - Server internal disk error.....              | 352 |
| 32302 - Server RAID disk error.....                  | 353 |
| 32303 - Server Platform error.....                   | 353 |
| 32304 - Server file system error.....                | 354 |
| 32305 - Server Platform process error.....           | 354 |
| 32306 - Server RAM shortage error.....               | 355 |
| 32307 - Server swap space shortage failure.....      | 355 |
| 32308 - Server provisioning network error.....       | 356 |
| 32309 - Eagle Network A Error.....                   | 356 |
| 32310 - Eagle Network B Error.....                   | 357 |
| 32311 - Sync Network Error.....                      | 357 |
| 32312 - Server disk space shortage error.....        | 358 |
| 32313 - Server default route network error.....      | 358 |
| 32314 - Server temperature error.....                | 359 |

|   |     |
|---|-----|
| 32315 - Server mainboard voltage error.....                   | 360 |
| 32316 - Server power feed error.....                          | 360 |
| 32317 - Server disk health test error.....                    | 361 |
| 32318 - Server disk unavailable error.....                    | 362 |
| 32319 - Device error.....                                     | 362 |
| 32320 - Device interface error.....                           | 363 |
| 32321 - Correctable ECC memory error.....                     | 363 |
| 32322 - Power Supply A error.....                             | 364 |
| 32323 - Power Supply B error.....                             | 364 |
| 32324 - Breaker panel feed error.....                         | 365 |
| 32325 - Breaker panel breaker error.....                      | 365 |
| 32326 - Breaker panel monitoring error.....                   | 368 |
| 32327 - Server HA Keepalive error.....                        | 369 |
| 32328 - DRBD is unavailable.....                              | 369 |
| 32329 - DRBD is not replicating.....                          | 370 |
| 32330 - DRBD peer problem.....                                | 370 |
| 32331 - HP disk problem.....                                  | 370 |
| 32332 - HP Smart Array controller problem.....                | 371 |
| 32333 - HP hpacucliStatus utility problem.....                | 371 |
| 32334 - Multipath device access link problem.....             | 372 |
| 32335 - Switch link down error.....                           | 373 |
| 32336 - Half Open Socket Limit.....                           | 373 |
| 32337 - Flash Program Failure.....                            | 374 |
| 32338 - Serial Mezzanine Unseated.....                        | 374 |
| 32339 - TPD Max Number Of Running Processes Error.....        | 374 |
| 32340 - TPD NTP Daemon Not Synchronized Error.....            | 375 |
| 32341 - TPD NTP Daemon Not Synchronized Error.....            | 376 |
| 32342 - NTP Offset Check Error.....                           | 377 |
| 32343 - TPD RAID disk .....                                   | 377 |
| 32344 - TPD RAID controller problem.....                      | 378 |
| 32345 - Server Upgrade snapshot(s) invalid.....               | 378 |
| 32346 - OEM hardware management service reports an error..... | 379 |
| 32347 - The hwmgmtcliStatus daemon needs intervention.....    | 379 |
| 32348 - FIPS subsystem problem.....                           | 380 |
| 32349 - File Tampering.....                                   | 380 |
| 32350 - Security Process Terminated.....                      | 381 |
| 32500 - Server disk space shortage warning.....               | 381 |
| 32501 - Server application process error.....                 | 382 |
| 32502 - Server hardware configuration error.....              | 382 |
| 32503 - Server RAM shortage warning.....                      | 383 |
| 32504 - Software Configuration Error.....                     | 383 |

|  |     |
|--|-----|
| 32505 - Server swap space shortage warning.....          | 383 |
| 32506 - Server default router not defined.....           | 384 |
| 32507 - Server temperature warning.....                  | 385 |
| 32508 - Server core file detected.....                   | 386 |
| 32509 - Server NTP Daemon not synchronized.....          | 386 |
| 32510 - CMOS battery voltage low.....                    | 387 |
| 32511 - Server disk self test warning.....               | 387 |
| 32512 - Device warning.....                              | 388 |
| 32513 - Device interface warning.....                    | 388 |
| 32514 - Server reboot watchdog initiated.....            | 389 |
| 32515 - Server HA failover inhibited.....                | 389 |
| 32516 - Server HA Active to Standby transition.....      | 390 |
| 32517 - Server HA Standby to Active transition.....      | 390 |
| 32518 - Platform Health Check failure.....               | 390 |
| 32519 - NTP Offset Check failure.....                    | 391 |
| 32520 - NTP Stratum Check failure.....                   | 392 |
| 32521 - SAS Presence Sensor Missing.....                 | 392 |
| 32522 - SAS Drive Missing.....                           | 393 |
| 32523 - DRBD failover busy.....                          | 393 |
| 32524 - HP disk resync.....                              | 394 |
| 32525 - Telco Fan Warning.....                           | 394 |
| 32526 - Telco Temperature Warning.....                   | 395 |
| 32527 - Telco Power Supply Warning.....                  | 395 |
| 32528 - Invalid BIOS value.....                          | 396 |
| 32529 - Server Kernel Dump File Detected.....            | 396 |
| 32530 - TPD Upgrade Failed.....                          | 396 |
| 32531 - Half Open Socket Warning Limit.....              | 397 |
| 32532 - Server Upgrade Pending Accept/Reject.....        | 397 |
| 32533 - TPD Max Number Of Running Processes Warning..... | 398 |
| 32534 - TPD NTP Source Is Bad Warning.....               | 398 |
| 32535 - TPD RAID disk resync.....                        | 399 |
| 32536 - TPD Server Upgrade snapshot(s) warning.....      | 399 |
| 32537 - FIPS subsystem warning event.....                | 400 |
| 32538 - Platform Data Collection Error.....              | 400 |
| 32539 - Server Patch Pending Accept/Reject.....          | 401 |
| 32540 - CPU Power limit mismatch.....                    | 401 |
| 32700 - Telco Switch Notification.....                   | 401 |
| 32701 - HIDS Initialized.....                            | 402 |
| 32702 - HIDS Baseline Deleted.....                       | 402 |
| 32703 - HIDS Enabled.....                                | 402 |
| 32704 - HIDS Disabled.....                               | 402 |

|  |     |
|--|-----|
| 32705 - HIDS Monitoring Suspended.....   | 403 |
| 32706 - HIDS Monitoring Resumed.....   | 403 |
| 32707 - HIDS Baseline Updated.....   | 403 |
| DM-IWF (33000-33024).....  | 403 |
| 33000 - MAP-to-Diameter Service Registration Failure on DA-MP.....                       | 404 |
| 33001 - Diameter-to-MAP Service Registration Failure on DA-MP.....                       | 404 |
| 33002 - DM-IWF DA-MP not associated with a Place.....                                    | 404 |
| 33003 - Insufficient memory for DM-IWF.....  | 405 |
| 33004 - DM-IWF Transaction Response Queue Utilization.....                               | 405 |
| 33005 - DM-IWF PTR Pool Utilization.....   | 406 |
| 33006 - MD-IWF Service Congestion.....   | 406 |
| 33007 - MD-IWF Error.....  | 407 |
| 33008 - DM-IWF maximum pending transactions allowed exceeded.....                        | 407 |
| 33009 - DM-IWF unexpected Answer response received from a SS7-MP.....                    | 408 |
| 33010 - MD-IWF ComAgent Connection exhausted.....  | 408 |
| 33011 - DM-IWF Answer Timeout.....   | 409 |
| 33012 - DM-IWF encode decode error.....  | 409 |
| 33013 - DRL queue exhaustion.....  | 409 |
| 33014 - Incompatible DA-MP Profile for DM-IWF.....                                       | 410 |
| 33015 - DM-IWF Diameter message size exceeded maximum supported size.....                | 411 |
| MD-IWF (33050-33099).....  | 411 |
| 33050 - MD-IWF Ingress Message Rate.....   | 411 |
| 33051 - MD-IWF Application Degraded or Unavailable.....                                  | 412 |
| 33052 - MD-IWF Notified that DM-IWF Service Status is Down.....                          | 412 |
| 33053 - MD-IWF DiamTrans Task Queue Utilization.....                                     | 413 |
| 33054 - MD-IWF MapTrans Task Queue Utilization.....                                      | 413 |
| 33055 - MD-IWF DAMPInterface Task Queue Utilization.....                                 | 414 |
| 33056 - MD-IWF ComAgent Provider Registration Failure on SS7-MP.....                     | 414 |
| 33057 - MD-IWF ComAgent User Registration Failure on SS7-MP.....                         | 415 |
| 33058 - MD-IWF DiamToMap PTR Utilization.....  | 415 |
| 33059 - MD-IWF MapToDiam PTR Utilization.....  | 416 |
| 33060 - SS7-MP Profile Not Assigned.....   | 416 |
| 33062 - Insufficient Memory for MD-IWF.....  | 416 |
| 33063 - MD-IWF SS7-MP not associated with a Place.....                                   | 417 |
| 33065 - MD-IWF Resource Exhaustion.....  | 417 |
| 33066 - MD-IWF orphan Diameter Answer message received.....                              | 418 |
| 33067 - MD-IWF orphan MAP Response message received.....                                 | 418 |
| 33068 - MD-IWF MAP Response timeout.....   | 419 |
| 33069 - MD-IWF Diameter Answer timeout.....  | 419 |
| 33070 - MD-IWF Generated Diameter Answer error message due to Diameter<br>Exception..... | 420 |

|   |     |
|---|-----|
| 33071 - MD-IWF Generated MAP Error Response due to MAP exception.....   | 420 |
| 33072 - MD-IWF received TCAP Notice from SS7 network.....   | 420 |
| 33073 - MD-IWF admin state set to Enabled.....  | 421 |
| 33074 - MD-IWF admin state set to Disabled.....   | 421 |
| 33075 - MD-IWF received ComAgent error or DM-IWF NACK.....  | 421 |
| 33076 - MD-IWF received Diameter Answer from unexpected DA-MP.....  | 422 |
| 33077 - MD-IWF address translation failed.....  | 422 |
| 33078 - MD-IWF received Diameter EIR message but Destination-Host AVP not<br>present or not found in mapping table..... | 423 |
| 33079 - MD-IWF message translation failed.....  | 423 |
| 33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter<br>message.....                                | 423 |
| GLA (33100-33149).....  | 424 |
| 33100 - GLA Message Decoding Failure.....   | 424 |
| 33101 - GLA Incorrect Application ID or Command Code.....   | 425 |
| 33102 - GLA Missing Subscriber ID.....  | 425 |
| 33103 - GLA Communication Agent Error.....  | 425 |
| 33104 - GLA Duplicate Subscriber ID.....  | 426 |
| 33105 - Routing Attempt failed due to queue exhaustion.....   | 426 |
| 33106 - GLA Communication Agent Timeout.....  | 427 |
| 33120 - Policy SBR Binding Sub-Resource Unavailable.....  | 427 |
| 33121 - GLA pSBR-B Response Task Message Queue Utilization.....   | 428 |
| Diameter Custom Applications (DCA) Framework Alarms and Events (33300-33630).....                                       | 428 |
| 33300 - Create Application Version Failure.....   | 428 |
| 33301 - Update Config Data Failure.....   | 429 |
| 33302 - Delete Application Version Failure.....   | 429 |
| 33303 - U-SBR Event Queue Utilization.....  | 429 |
| 33304 - DCA Runtime Errors.....   | 430 |
| 33305 - DCA Procedure Not Found.....  | 431 |
| 33306 - U-SBR Resolution Failure.....   | 431 |
| 33307 - Diameter Message Routing Failure Due To Full DRL Queue.....   | 432 |
| 33308 - DCA to U-SBR ComAgent Error.....  | 432 |
| 33309 - DCA Script Compilation Error.....   | 432 |
| 33310 - U-SBR Sub-resource Unavailable.....   | 433 |
| 33311 - DCA Application Reloaded.....   | 433 |
| 33312 - DCA Script Generation Error.....  | 434 |
| 33313 - DCA U-SBR Logical Name Mismatch.....  | 434 |
| 33314 - Custom MEAL differentiation error.....  | 434 |
| DCA Custom MEAL Event Templates.....  | 435 |
| Independent SBR Alarms and Events (33730-33830).....  | 436 |
| 33730 - U-SBR Database Audit Statistics Report.....   | 436 |

|   |            |
|---|------------|
| <b>Chapter 5: Key Performance Indicators (KPIs)</b> ..... | <b>437</b> |
| General KPIs information.....                             | 438        |
| KPIs overview.....  | 438        |
| KPIs.....   | 438        |
| KPIs server elements .....                                | 438        |
| Viewing KPIs.....   | 439        |
| KPIs data export elements.....                            | 439        |
| Exporting KPIs.....                                       | 440        |
| Computer Aided Policy Making (CAPM) KPIs.....             | 441        |
| Communication Agent (ComAgent) KPIs.....                  | 441        |
| Diameter (DIAM) KPIs.....                                 | 442        |
| DM-IWF KPIs.....  | 442        |
| GLA KPIs.....   | 442        |
| IDIH KPIs.....  | 443        |
| IP Front End (IPFE) KPIs.....                             | 443        |
| MD-IWF KPIs.....  | 444        |
| Message Processor (MP) KPIs.....                          | 444        |
| Full Address Based Resolution (FABR) KPIs.....            | 445        |
| Platform KPIs.....  | 445        |
| Policy and Charging Application (PCA) KPIs.....           | 446        |
| Range Based Address Resolution (RBAR) KPIs.....           | 446        |
| Subscriber Binding Repository (SBR) KPIs.....             | 447        |
| SS7/Sigtran KPIs.....                                     | 448        |
| DCA Framework KPIs.....                                   | 448        |
| DCA Custom MEAL KPIs.....                                 | 449        |
| U-SBR KPIs.....   | 449        |
| <b>Glossary</b> .....                                     | <b>451</b> |

# List of Figures

Figure 1: Oracle System Login.....41

Figure 2: Paginated Table.....43

Figure 3: Scrollable Table.....44

Figure 4: Form Page.....44

Figure 5: Tabbed Pages.....45

Figure 6: Tabbed Pages.....45

Figure 7: Report Output.....45

Figure 8: Sorting a Table by Column Header.....46

Figure 9: Clear Field Control X.....47

Figure 10: Optional Layout Element Toolbar.....47

Figure 11: Automatic Error Notification.....48

Figure 12: Examples of Filter Styles.....49

Figure 13: Flow of Alarms.....54

Figure 14: Alarm Indicators Legend.....54

Figure 15: Trap Count Indicator Legend.....55

Figure 16: Breaker Panel LEDs.....366

Figure 17: Breaker Panel Setting.....367

# List of Tables

|   |     |
|---|-----|
| Table 1: Admonishments.....                               | 29  |
| Table 2: User Interface Elements.....                     | 34  |
| Table 3: Main Menu Options.....                           | 35  |
| Table 4: Main Menu Icons.....                             | 42  |
| Table 5: Example Action Buttons.....                      | 46  |
| Table 6: Submit Buttons.....                              | 47  |
| Table 7: Filter Control Elements.....                     | 49  |
| Table 8: Alarm/Event ID Ranges.....                       | 55  |
| Table 9: Alarm and Event Types.....                       | 56  |
| Table 10: Schedule Active Alarm Data Export Elements..... | 58  |
| Table 11: Schedule Event Data Export Elements.....        | 61  |
| Table 12: Data Export Elements.....                       | 64  |
| Table 13: Active Tasks Elements.....                      | 67  |
| Table 14: Active Tasks Report Elements.....               | 70  |
| Table 15: Scheduled Tasks Elements.....                   | 71  |
| Table 16: KPIs Server Elements.....                       | 438 |
| Table 17: Schedule KPI Data Export Elements.....          | 439 |
| Table 18: CAPM KPIs.....                                  | 441 |
| Table 19: Communication Agent KPIs.....                   | 441 |
| Table 20: DIAM KPIs.....                                  | 442 |
| Table 21: DM-IWF KPIs.....                                | 442 |
| Table 22: IPFE KPIs.....                                  | 443 |

|                                 |     |
|---------------------------------|-----|
| Table 23: MP KPIs.....          | 444 |
| Table 24: FABR KPIs.....        | 445 |
| Table 25: Platform KPIs.....    | 445 |
| Table 26: PCA KPIs.....         | 446 |
| Table 27: RBAR KPIs.....        | 446 |
| Table 28: SBR KPIs.....         | 447 |
| Table 29: SBR-Binding KPIs..... | 447 |
| Table 30: SBR-Session KPIs..... | 447 |
| Table 31: SS7/Sigtran KPIs..... | 448 |

# Chapter 1

## Introduction

---

### Topics:

- *Revision History.....28*
- *Overview.....28*
- *Scope and Audience.....28*
- *Manual Organization.....28*
- *Documentation Admonishments.....29*
- *Related Specifications.....29*
- *Locate Product Documentation on the Oracle Help Center Site.....30*
- *Customer Training.....30*
- *My Oracle Support (MOS).....30*
- *Emergency Response.....31*

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 | <ul style="list-style-type: none"> <li>• New alarms and events added for new features, DCA, U-SBR, I-SBR, and COMCOL.</li> <li>• KPIs added for DCA and U-SBR.</li> </ul> |

## Overview

The *DSR Alarms and KPIs* documentation provides information about DSR alarms, events, and KPIs provides corrective maintenance procedures, and other information used in maintaining the system.

- Information relevant to understanding alarms and events that may occur on 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
- The procedure for viewing KPIs
- Lists 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 will aid personnel in maintaining the DSR.

The corrective maintenance procedures are those used in response to a system alarm or output message. These procedures are used to aid in the detection, isolation, and repair of 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 \(MOS\)](#), and [Locate Product Documentation on the Oracle Help Center Site](#).
- *User Interface Introduction* describes the organization and usage of the application 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.

- [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, then numerically by the number that appears 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: Admonishments**

| Icon   | Description   |
|--|---|
| <br>DANGER    | Danger:<br>(This icon and text indicate the possibility of <i>personal injury</i> .)                      |
| <br>WARNING | Warning:<br>(This icon and text indicate the possibility of <i>equipment damage</i> .)                    |
| <br>CAUTION | Caution:<br>(This icon and text indicate the possibility of <i>service interruption</i> .)                |
| <br>TOPPLE  | Topple:<br>(This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .) |

## Related Specifications

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

## Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.  
The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.  
A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

## Customer Training

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

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

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

[www.oracle.com/education/contacts](http://www.oracle.com/education/contacts)

## My Oracle Support (MOS)

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

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

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

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS 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.

## User Interface Introduction

---

### Topics:

- [User Interface Organization.....33](#)
- [Missing Main Menu options.....40](#)
- [Common Graphical User Interface Widgets.....40](#)

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
- Alarm and Events
- Security Log
- Status & 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 appear on the Network OAM GUI:

- Communication Agent
- Diameter Common
- Diameter
- UDR
- Policy and Charging
- MAP-Diameter IWF
- SBR
- RADIUS
- DCA 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
- FABR
- IPFE
- GLA
- Policy and Charging
- MAP-Diameter IWF
- SBR
- RADIUS
- Mediation
- DCA Framework

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

## User Interface Elements

[Table 2: User Interface Elements](#) describes elements of the user interface.

**Table 2: User Interface Elements**

| Element               | Location                                | Function  |
|-----------------------|---|---|
| Identification Banner | Top bar across the web page             | Displays the company name, product name and version, and the alarm panel.   |
| Session Banner        | Next bar across the top of the web page | <p>The left side of the banner just above the Main Menu provides the following session information:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• The HA state of the machine to which the user is connected.</li> <li>• The role of the machine to which the user is connected.</li> </ul> <p>The right side of the banner:</p> <ul style="list-style-type: none"> <li>• Shows the user name of the currently logged-in user.</li> <li>• Provides a link to log out of the GUI.</li> </ul>   |
| Main Menu             | Left side of screen, under banners      | <p>A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders.</p> <ul style="list-style-type: none"> <li>• To display submenu items, click the plus character, the folder, or anywhere on the same line.</li> <li>• To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.</li> </ul>  |
| Work Area             | Right side of panel under status        | <p>Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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 <a href="#">Optional Layout Element Toolbar</a>.</li> </ul> |

| Element | Location | Function   |
|---------|----------|--|
|         |          | <ul style="list-style-type: none"> <li>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 user interface page. The page displays a user-defined welcome message. To customize the message, see <a href="#">Customizing the Login Message</a>.</li> </ul> |

## Main Menu Options

*Table 3: Main Menu Options* describes all main menu user interface options.

**Note:** The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options do not appear 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 appear in the main menu until the features are activated.

**Table 3: Main Menu Options**

| Menu Item      | Function   |
|----------------|--|
| Administration | <p>The Administration menu allows the user to:</p> <ul style="list-style-type: none"> <li>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</li> <li>Set up and manage user accounts</li> <li>Configure group permissions</li> <li>View session information</li> <li>Manage sign-on certificates</li> <li>Authorize IP addresses to access the user interface</li> <li>Configure SFTP user information</li> <li>View the software versions report</li> <li>Upgrade management including backup and reporting</li> <li>Authenticate LDAP servers</li> <li>Configure SNMP trapping services</li> <li>Configure an export server</li> <li>Configure DNS elements</li> </ul> |
| Configuration  | <p>On the NOAM, allows the user to configure:</p> <ul style="list-style-type: none"> <li>Network Elements</li> </ul>   |

| Menu Item                      | Function   |
|--------------------------------|--|
|                                | <ul style="list-style-type: none"> <li>• Network Devices</li> <li>• Network Routes</li> <li>• Services</li> <li>• Servers</li> <li>• Server Groups</li> <li>• Resource Domains</li> <li>• Places</li> <li>• Place Associations</li> <li>• Interface and Port DSCP</li> </ul>   |
| Alarms and Events              | <p>Allows the user to view:</p> <ul style="list-style-type: none"> <li>• Active alarms and events</li> <li>• Alarm and event history</li> <li>• Trap log</li> </ul>  |
| Security Log                   | <p>Allows the user to view, export, and generate reports from security log history.</p>  |
| Status & Manage                | <p>Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, KPIs, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.</p>   |
| Measurements                   | <p>Allows the user to view and export measurement data.</p>  |
| Transport Manager (optional)   | <p>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 appears with the DSR application.</p>  |
| Communication Agent (optional) | <p>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.</p>   |
| SS7/Sigtran (optional)         | <p>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 appears with the DSR application.</p>   |
| Diameter Common (optional)     | <p>Allows the user to view or configure:</p> <ul style="list-style-type: none"> <li>• Dashboard, configure on the NOAM; view on both OAMs</li> <li>• Network Identifiers on the SOAM - MCC Ranges</li> <li>• Network Identifiers on the NOAM - MCCMNC and MCCMNC Mapping</li> <li>• MPs (on the SOAM) - editable Profile parameters and Profile Assignments</li> </ul> <p>The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.</p> |

| Menu Item  | Function   |
|--|--|
| Diameter (optional)                              | <p>Allows the user to configure, modify, and monitor Diameter routing:</p> <ul style="list-style-type: none"> <li>• On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration</li> <li>• On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with IDIH, AVP Dictionary, and Diameter Mediation configuration</li> </ul>   |
| UDR (optional)                                   | <p>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 appears with the UDR application.</p>   |
| RBAR (Range-Based Address Resolution) (optional) | <p>Allows the user to configure the following Range-Based Address Resolution (RBAR) settings:</p> <ul style="list-style-type: none"> <li>• Applications</li> <li>• Exceptions</li> <li>• Destinations</li> <li>• Address Tables</li> <li>• Addresses</li> <li>• Address Resolutions</li> <li>• System Options</li> </ul> <p>This is accessible from the SOAM only. This option only appears with the DSR application.</p>  |
| FABR (Full Address Based Resolution) (optional)  | <p>Allows the user to configure the following Full Address Based Resolution (FABR) settings:</p> <ul style="list-style-type: none"> <li>• Applications</li> <li>• Exceptions</li> <li>• Default Destinations</li> <li>• Address Resolutions</li> <li>• System Options</li> </ul> <p>This is accessible from the SOAM only. This option is only available with the DSR application.</p>   |
| Policy and Charging (optional)                   | <p>On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> <li>• General Options</li> <li>• Access Point Names</li> <li>• Policy DRA <ul style="list-style-type: none"> <li>• PCRF Pools</li> <li>• PCRF Sub-Pool Selection Rules</li> <li>• Network-Wide Options</li> </ul> </li> <li>• Online Charging DRA <ul style="list-style-type: none"> <li>• OCS Session State</li> <li>• Realms</li> </ul> </li> </ul> |

| Menu Item                               | Function  |
|---|---|
|   | <ul style="list-style-type: none"> <li>• Network-Wide Options</li> <li>• Alarm Settings</li> <li>• Congestion Options</li> </ul> <p>Additionally on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> <li>• Maintenance                             <ul style="list-style-type: none"> <li>• SBR Database Status</li> <li>• SBR Status</li> <li>• SBR Database Reconfiguration Status</li> <li>• Policy Database Query</li> </ul> </li> </ul> <p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> <li>• General Options</li> <li>• Access Point Names</li> <li>• Policy DRA                             <ul style="list-style-type: none"> <li>• PCRFs</li> <li>• Binding Key Priority</li> <li>• PCRF Pools</li> <li>• PCRF Pool to PRT Mapping</li> <li>• PCRF Sub-Pool Selection Rules</li> <li>• Policy Clients</li> <li>• Suspect Binding Removal Rules</li> <li>• Site Options</li> </ul> </li> <li>• Online Charging DRA                             <ul style="list-style-type: none"> <li>• OCSs</li> <li>• CTFs</li> <li>• OCS Session State</li> <li>• Realms</li> </ul> </li> <li>• Error Codes</li> <li>• Alarm Settings</li> <li>• Congestion Options</li> </ul> <p>This option only appears with the DSR application.</p> |
| Gateway Location Application (optional) | <p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> <li>• Exceptions</li> <li>• Options</li> </ul> <p>GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP). This option only appears with the DSR application.</p>  |

| Menu Item                            | Function  |
|--------------------------------------|---|
| IPFE (optional)                      | <p>Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only. This option only appears with the DSR application.</p>  |
| MAP-Diameter Interworking (optional) | <p>On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application:</p> <ul style="list-style-type: none"> <li>• DM-IWF Options</li> <li>• Diameter Exception</li> </ul> <p>On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application:</p> <ul style="list-style-type: none"> <li>• MD-IWF Options</li> <li>• Diameter Realm</li> <li>• Diameter Identity GTA</li> <li>• GTA Range to PC</li> <li>• MAP Exception</li> <li>• CCNDC Mapping</li> </ul> <p>This option only appears with the DSR application.</p>                              |
| RADIUS (optional)                    | <p>Allows the user to perform configuration tasks, edit system options, and view elements for:</p> <ul style="list-style-type: none"> <li>• Network Options</li> <li>• Message Authenticator Configuration Sets</li> <li>• Shared Secret Configuration Sets</li> <li>• Ingress Status Server Configuration Sets</li> <li>• Message Conversion Configuration Sets</li> <li>• NAS Node</li> </ul> <p>This option only appears with the DSR application.</p>   |
| SBR (optional)                       | <p>Allows the user to perform configuration tasks, edit system options, and view elements for:</p> <ul style="list-style-type: none"> <li>• SBR Databases</li> <li>• SBR Database Resizing Plans</li> <li>• SBR Data Migration Plans</li> <li>• Database Options</li> </ul> <p>Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:</p> <ul style="list-style-type: none"> <li>• Maintenance <ul style="list-style-type: none"> <li>• SBR Database Status</li> <li>• SBR Status</li> <li>• SBR Database Reconfiguration Status</li> </ul> </li> </ul> <p>This option only appears with the DSR application.</p> |

| Menu Item                | Function  |
|--------------------------|---|
| DCA Framework (optional) | Allows the user to perform configuration tasks, edit system options, and view elements for DCA applications: <ul style="list-style-type: none"> <li>• Custom MEALs</li> <li>• General Options</li> <li>• Trial MPs assignment</li> <li>• Application Control</li> <li>• System Options</li> </ul> |
| 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 appear 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.

## 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 appears 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 appears. You can create a login message that appears just below the **Log In** button on the **System Login** page.



**ORACLE®**

**Oracle System Login** Wed Jul 8 14:20:00 2015 EDT

**Log In**  
Enter your username and password to log in

Username:

Password:

Change password

Welcome to the Oracle System Login.

Unauthorized access is prohibited. This Oracle system requires the use of Microsoft Internet Explorer 8.0, 9.0, or 10.0 with support for JavaScript and cookies.

---

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

Copyright © 2010, 2015, [Oracle](#) and/or its affiliates. All rights reserved.

**Figure 1: Oracle System Login**

1. From the **Main Menu**, click **Administration > General Options**.

The **General Options Administration** page appears.

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 appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to 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 then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

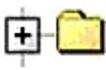
1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example `https://dsr-no.yourcompany.com`.  
When using Single Sign-On, you cannot use the IP address of the server.
2. When prompted by the browser, confirm that the server can be trusted.  
The System Login page appears.
3. Enter the Username and Password for your account.  
The DSR GUI for the NOAM appears.
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 appears

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 4: 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. |
|  | 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.  |

| Icon   | Name                    | Description                              |
|--|-------------------------|--|
|   | 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](#).

Displaying Records 1-1 of 1 | [First](#) | [Prev](#) | [Next](#) | [Last](#)

| Action                                      | System ID | IP Address | Permission | Action                                      |
|---|-----------|------------|------------|---|
| <a href="#">Edit</a> <a href="#">Delete</a> | lisa      | 10.25.62.4 | READ_WRITE | <a href="#">Edit</a> <a href="#">Delete</a> |

Displaying Records 1-1 of 1 | [First](#) | [Prev](#) | [Next](#) | [Last](#)

**Figure 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](#).

| Sequence # | Alarm ID | Timestamp                    | Severity | Product    | Process    | NE     | Server      | Type | Instance    | Alarm Text   |
|------------|----------|------------------------------|----------|------------|------------|--------|-------------|------|-------------|--|
| 3498       | 31201    | 2009-Jun-11 18:07:41.214 UTC | MAJOR    | MiddleWare | procmgr    | OAMPNE | teks8011006 | PROC | eclipseHelp | A managed process cannot be started or has unexpectedly terminated |
| 5445       | 31201    | 2009-Jun-11 18:07:27.137 UTC | MAJOR    | MiddleWare | procmgr    | SOAMP  | teks8011002 | PROC | eclipseHelp | A managed process cannot be started or has unexpectedly terminated |
| 5443       | 31107    | 2009-Jun-11 18:07:24.704 UTC | MINOR    | MiddleWare | inetmerge  | SOAMP  | teks8011002 | COLL | teks8011004 | DB merging from a child Source Node has failed                     |
| 5444       | 31107    | 2009-Jun-11 18:07:24.704 UTC | MINOR    | MiddleWare | inetmerge  | SOAMP  | teks8011002 | COLL | teks8011003 | DB merging from a child Source Node has failed                     |
| 5441       | 31209    | 2009-Jun-11 18:07:22.640 UTC | MINOR    | MiddleWare | re.portmap | SOAMP  | teks8011002 | SW   | teks8011003 | Unable to resolve a hostname specified in the Nodeinfo table.      |
|            |          |                              |          |            |            |        |             |      |             | Unable to resolve a  |

Export

Figure 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 pulldown lists, buttons, and links.

Username:  (5-16 characters)

Group:

Time Zone:

Maximum Concurrent Logins:  Maximum concurrent logins for a user (0=no limit). [Default = 1; Range = 0-50]

Session Inactivity Limit:  Time (in minutes) after which login sessions expire (0 = never). [Default = 120; Range = 0-120]

Comment:  (max 64 characters)

Temporary Password:  (8-16 characters)

Re-type Password:

Ok Apply Cancel

Figure 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.

|                       |                  |                                   |                                |                                    |                                 |                                   |
|-----------------------|------------------|-----------------------------------|--------------------------------|------------------------------------|---------------------------------|-----------------------------------|
| <b>Entire Network</b> | *                | System.CPU_CoreUtilPct_Average    | System.CPU_CoreUtilPct_Peak    |                                    |                                 |                                   |
| <b>NOAMP</b>          |                  |                                   |                                |                                    |                                 |                                   |
| <b>SOAM</b>           |                  |                                   |                                |                                    |                                 |                                   |
|                       | <b>Timestamp</b> | <b>System CPU UtilPct Average</b> | <b>System CPU UtilPct Peak</b> | <b>System Disk UtilPct Average</b> | <b>System Disk UtilPct Peak</b> | <b>System RAM UtilPct Average</b> |
|                       | 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 5: Tabbed Pages

Retrieve Add Update Delete

Fields marked with a red asterisk (\*) require a value.

| Field          | Value                | Description  |
|----------------|----------------------|--|
| Network Entity | <input type="text"/> | * Numeric identifier for the Network Entity<br>1-15 DIGITS |

Retrieve

Figure 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.

```

=====
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
=====

```

Figure 7: Report Output

## Customizing the Splash Page Welcome Message

When you first log in to the user interface, the splash page appears. 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 appears at the top of the page to inform you if the operation was successful.

The next time you log in to the user interface, the new welcome message text is displayed.

## 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 that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See [Figure 8: Sorting a Table by Column Header](#). Clicking the column header again reverses the direction of the sort.

| Local Node Name | Realm | FQDN | SCTP Listen Port | TCP Listen Port | Connection Configuration Set | CEX Configuration Set | IP Addresses |
|-----------------|-------|------|------------------|-----------------|------------------------------|-----------------------|--------------|
|-----------------|-------|------|------------------|-----------------|------------------------------|-----------------------|--------------|

Figure 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 5: Example Action Buttons](#) contains examples of Action buttons.

Table 5: Example Action Buttons

| Action Button | Function                   |
|---------------|----------------------------|
| Insert        | Inserts data into a table. |
| Edit          | Edits data within a table. |
| Delete        | Deletes data from table.   |

| Action Button | Function                                |
|---------------|---|
| Change        | Changes the status of a managed object. |

Some Action buttons take you to another page.

Submit buttons, described in [Table 6: Submit Buttons](#), 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 6: 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 pulldown list. The clear field control is available only on some pulldown fields.

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



**Figure 9: Clear Field Control X**

## Optional Layout Element Toolbar

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



**Figure 10: Optional Layout Element Toolbar**

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear 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 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 12: Examples of Filter Styles

### Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: 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.             |
| >=       | 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 <b>Is Null</b> 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** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

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 pulldown menu.  
The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
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. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Click **Filter** in the optional layout element toolbar.
2. Select a field name from the **Display Filter** pulldown menu.  
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.  
The selected field name displays in the **Display Filter** field.
3. Select an operator from the operation selector pulldown menu.
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. For data tables that support compound filtering, click **Add** to add another filter condition. Then repeat steps 2 through 4.  
Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

## 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.

# Chapter 3

## Alarms, Events, and KPIs Overview

---

### Topics:

- [Help Organization.....53](#)
- [Alarms Warning.....53](#)
- [General alarms and events information.....53](#)
- [Viewing the file list.....63](#)
- [Opening a file.....64](#)
- [Data Export.....64](#)
- [Tasks.....67](#)

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

## Help Organization

Information in this document is organized into the following sections:

- [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, then numerically by the number that appears in the application.
- [Key Performance Indicators \(KPIs\)](#) provides detailed KPI information, organized alphabetically by KPI name.

## 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 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 13: Flow of Alarms shows how Alarms and Events are organized in the application.

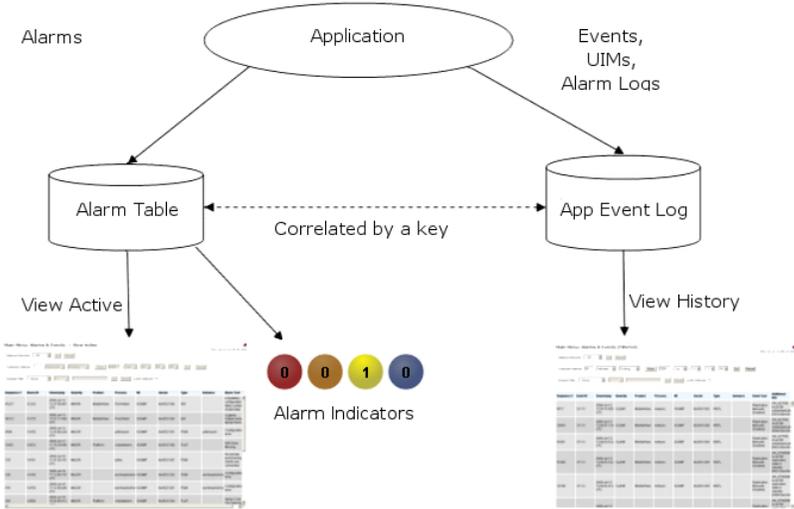


Figure 13: Flow of Alarms

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.

|  |                                     |
|--|-------------------------------------|
|  | Active Critical Alarm (bright red)  |
|  | Active Major Alarm (bright orange)  |
|  | Active Minor Alarm (bright yellow)  |
|  | No active Critical Alarm (pale red) |
|  | No active Major Alarm (pale orange) |
|  | No active Minor Alarm (pale yellow) |
|  | Not Connected (white)               |

Figure 14: Alarm Indicators Legend

|   |                                 |
|---|---------------------------------|
|  | Trap count > 0<br>(bright blue) |
|  | Trap count = 0<br>(pale blue)   |

Figure 15: 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 following process classifications:

Table 8: 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                                     |

| Application/Process Name | Alarm ID Range |
|--------------------------|----------------|
| 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

This table describes the possible alarm/event types that can be displayed.

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

**Table 9: 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                             |

| Type Name | Type                                     |
|-----------|--|
| ERA       | Event Responder Application              |
| FABR      | Full Address Based Resolution            |
| HA        | High Availability                        |
| HTTP      | Hypertext Transfer Protocol              |
| IDIH      | Integrated DIH                           |
| IF        | Interface                                |
| IP        | Internet Protocol                        |
| IPFE      | IP Front End                             |
| LOADGEN   | Load Generator                           |
| LOG       | Logging                                  |
| MEAS      | Measurements                             |
| MEM       | Memory                                   |
| NAT       | Network Address Translation              |
| NP        | Number Portability                       |
| OAM       | Operations, Administration & Maintenance |
| PCRF      | Policy Charging Rules Function           |
| PDRA      | Policy Diameter Routing Agent            |
| PLAT      | Platform                                 |
| PROC      | Process                                  |
| PROV      | Provisioning                             |
| pSBR      | Policy SBR                               |
| QP        | QBus                                     |
| RBAR      | Range-Based Address Resolution           |
| REPL      | Replication                              |
| SCTP      | Stream Control Transmission Protocol     |
| SDS       | Subscriber Database Server               |
| SIGC      | Signaling Compression                    |
| SIP       | Session Initiation Protocol Interface    |
| SL        | Selective Logging                        |
| SS7       | Signaling System 7                       |
| SSR       | SIP Signaling Router                     |

| Type Name | Type                          |
|-----------|-------------------------------|
| 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. Select **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 10: Schedule Active Alarm Data Export Elements**

| Element     | Description                       | Data Input Notes   |
|-------------|-----------------------------------|--|
| Task Name   | Name of the scheduled task        | Format: Textbox<br>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<br>Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign  |

| Element          | Description  | Data Input Notes  |
|------------------|--|---|
|                  |  | (-). Description must begin with an alphanumeric character.   |
| Export Frequency | Frequency at which the export occurs   | Format: Option<br>Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly<br>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<br>Range: 0 to 59<br>Default: 0  |
| Time of Day      | Time of day the export occurs  | Format: Time textbox<br>Range: 15-minute increments<br>Default: 12:00 AM                                      |
| Day of Week      | Day of week on which the export occurs   | Format: Option<br>Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday<br>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.



• The active alarms are now available in Alarms\_20090812\_180627.csv.

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. Select **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. Select **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 11: Schedule Event Data Export Elements**

| Element          | Description                          | Data Input Notes   |
|------------------|--------------------------------------|--|
| Task Name        | Name of the scheduled task           | Format: Textbox<br>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<br>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<br>Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily  |

| Element     | Description  | Data Input Notes   |
|-------------|--|--|
|             |  | 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<br>Range: 0 to 59<br>Default: 0   |
| Time of Day | Time of day the export occurs  | Format: Time textbox<br>Range: 15-minute increments<br>Default: 12:00 AM                                       |
| Day of Week | Day of week on which the export occurs   | Format: Options<br>Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday<br>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. Select **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 12: Data Export Elements**

| Element  | Description           | Data Input Notes  |
|----------|-----------------------|---|
| Hostname | Name of export server | Must be a valid hostname or a valid IP address.<br><br>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. |

| Element                        | Description  | Data Input Notes   |
|--------------------------------|--|--|
|                                |  | <p>To clear the current export server and remove the file transfer task, specify an empty hostname and username.</p> <p>Default: None</p>  |
| Username                       | Username used to access the export server  | <p>Format: Textbox</p> <p>Range: Maximum length is 32 characters; alphanumeric characters (a-z, A-Z, and 0-9).</p> <p>To clear the current export server and remove the file transfer task, specify an empty hostname and username.</p> <p>Default: None</p>         |
| Directory on Export Server     | Directory path on the export server where the exported data files are to be transferred              | <p>Format: Textbox</p> <p>Range: Maximum length is 255 characters; valid value is any UNIX string.</p> <p>Default: None</p>  |
| Path to rsync on Export Server | Optional path to the rsync binary on the export server   | <p>Format: Textbox</p> <p>Range: Maximum length is 4096 characters; alphanumeric characters (a-z, A-Z, and 0-9),dash, underscore, period, and forward slash.</p> <p>Default: If no path is specified, the username's home directory on the export server is used</p> |
| Backup File Copy Enabled       | Enables or disables the transfer of the backup files   | <p>Format: Checkbox</p> <p>Default: Disabled (unchecked)</p>   |
| File Compression               | Compression algorithm used when exported data files are initially created on the local host          | <p>Format: Radio button</p> <p>Range: gzip, bzip2, or none</p> <p>Default: gzip</p>  |
| Upload Frequency               | Frequency at which the export occurs   | <p>Format: Radio button</p> <p>Range: fifteen minutes, hourly, daily or weekly</p> <p>Default: weekly</p>  |
| Minute                         | If The Upload Frequency is Hourly, this is the minute of each hour when the transfer is set to begin | <p>Format: Scrolling list</p> <p>Range: 0 to 59</p> <p>Default: zero</p>   |
| Time of Day                    | If the Upload Frequency is Daily of Weekly, this is the time of day the export occurs                | <p>Format: Time textbox</p> <p>Range: HH:MM AM/PM in 15-minute increments</p>  |

| Element          | Description   | Data Input Notes  |
|------------------|---|---|
|                  |   | 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: Radio button<br>Range: Sunday through Saturday<br>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 [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. This table describes elements on the **Active Tasks** page.

**Table 13: Active Tasks Elements**

| Active Tasks Element | Description |
|----------------------|-------------|
| ID                   | Task ID     |
| Name                 | Task name   |

| Active Tasks Element | Description  |
|----------------------|--|
| 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. Select **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. Select **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. Select **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. Select **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. Select **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. This table describes elements on the **Active Tasks [Report]** page.

Table 14: Active Tasks Report Elements

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

### Generating an active task report

Use this procedure to generate an active task report.

1. Select **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.

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. This table describes elements on the **Scheduled Tasks** page.

**Table 15: 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. Select **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. Select **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. Select **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.

# Chapter 4

## Alarms and Events

---

### Topics:

- *IP Front End, IPFE (5000-5999).....75*
- *OAM (10000-10999).....83*
- *IDIH (11500-11549).....106*
- *SS7/Sigtran Alarms (19200-19299).....110*
- *Transport Manager Alarms and Events (19400-19419).....140*
- *Communication Agent, ComAgent (19420-19909).....148*
- *Diameter Signaling Router (DSR) Diagnostics (19910-19999).....180*
- *Diameter Alarms and Events (8000-8299, 22000-22350, 22900-22999, 25500-25899).....181*
- *Range Based Address Resolution (RBAR) Alarms and Events (22400-22424).....261*
- *Generic Application Alarms and Events (22500-22599).....265*
- *Full Address Based Resolution (FABR) Alarms and Events (22600-22640).....269*
- *Policy and Charging Application (PCA) Alarms and Events (22700-22799).....275*
- *Tekelec Virtual Operating Environment, TVOE (24400-24499).....296*
- *Computer Aided Policy Making, CAPM (25000-25499).....297*
- *OAM Alarm Management (25500-25899).....301*
- *Platform (31000-32800).....304*
- *DM-IWF (33000-33024).....403*
- *MD-IWF (33050-33099).....411*
- *GLA (33100-33149).....424*
- *Diameter Custom Applications (DCA) Framework Alarms and Events (33300-33630).....428*

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.

- *Independent SBR Alarms and Events*  
(33730-33830).....436



## 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

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | IPFE   |
| <b>Description:</b>        | The IPFE has not received any heartbeats from an application server within the heartbeat timeout interval. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | IP address of the application server.  |
|                            | <b>Note:</b> If a heartbeat is received from the application server, this alarm will clear.                |
| <b>HA Score:</b>           | Degraded   |
| <b>Auto Clear Seconds:</b> | N/A  |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

### 5002 - IPFE address configuration error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | IPFE   |
| <b>Description:</b>        | This alarm indicates misconfiguration due to manual changes to the configuration database, configuration data importing errors, or software installation errors. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | Description of the field or fields that are incorrect.   |
|                            | <b>Note:</b> If the IPFE is able to successfully synchronize data with its peer, this alarm will clear.  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | N/A  |
| <b>OID:</b>                | ipfeIpfeStateSyncConfigErrorNotify   |

**Recovery:**

1. To correct configuration errors, select **IPFE > Configuration > Options** from the left-hand menu.  
The **Configuration Options** pane appears.
2. Ensure that IPFE1 IP Address and IPFE2 IP Address are configured correctly.
3. For issues with modules or versions, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**5003 - IPFE state sync run error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | The IPFE was unable to synchronize state data with its mate.  |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | One of the following strings: <ul style="list-style-type: none"> <li>• "connect error" - cannot connect to peer IPFE</li> <li>• "data read error" - error reading data from peer IPFE</li> <li>• "data write error" - error writing data to peer IPFE</li> </ul> <p><b>Note:</b> If the is able to synchronize state data with its mate, this alarm will clear.</p> |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | N/A   |
| <b>OID:</b>                | ipfeIpfeStateSyncRunErrorNotify   |

**Recovery:**

1. Check the status of the peer IPFE by navigating to the **Status & Manage > Server** page.
2. If the IPFE is down, restart the process:
  - a) Select **Status & Manage > Server**. The **Server Status** page appears.
  - b) Click to select the IPFE to restart.
  - c) Click **Restart**.

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

- d) Click **OK** to continue.
3. Diagnose any network fault between the two IPFEs.
  4. For further assistance, it is recommended to contact [My Oracle Support \(MOS\)](#).

**5004 - IPFE IP tables configuration error**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | IPFE  |
| <b>Description:</b> | This alarm indicates misconfiguration of the Target Set due to manual changes to the configuration database or configuration data importing errors. |

|                            |  |
|----------------------------|--|
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | "tsa N address misconfiguration" where N is 1-16 |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | N/A  |
| <b>OID:</b>                | ipfeIpfeIpTablesConfigErrorNotify                |

**Recovery:**

1. Select **IPFE > Configuration > Options** from the left-hand menu.

**Note:** When the target set address is configured correctly, this alarm will clear.

The **Configuration Options** pane appears.

2. Ensure that the **TSA1 IP Address** field contains a valid IP address.
3. Select **IPFE > Configuration > IP List TSA 1**.

The **IP List TSA 1** pane appears.

4. Ensure that there is at least one application server IP address configured for the TSA.
5. Repeat for **IPFE > Configuration > IP List TSA 1**.

**5005 - IPFE Backend In Stasis**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | IPFE   |
| <b>Description:</b>        | <p>The IPFE has received a heartbeat packet from the application server that indicates that the application server is unwilling to accept new connections. However, the application server will continue to process existing connections. The application server sends a stasis heartbeat message for the following reasons:</p> <ul style="list-style-type: none"> <li>• The application server has reached its maximum number of active Diameter connections</li> <li>• The application server is congested. The application server will raise <a href="#">22200 - MpCpuCongested</a> also.</li> </ul> |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | IP address of the application server in stasis   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | N/A  |
| <b>OID:</b>                | ipfeIpfeBackendInStasisNotify  |

**Recovery:**

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

**5006 - Error reading from Ethernet device. Restart IPFE process.****Alarm Group:** IPFE**Description:** The IPFE was unable to read from an ethernet device.**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:** If the IPFE is able to read from the ethernet device, this alarm clears.

1. Select **Status & Manage > Server**.

The Server Status page appears.

2. Click to select the IPFE to restart.

3. Click **Restart**.

A warning message appears:

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

4. Click **OK** to continue.

**5007 - Out of Balance: Low****Alarm Group:** IPFE**Description:** Traffic statistics reveal that an application server is processing higher 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 will receive no traffic and thus will be considered "underloaded".**Severity:** Minor**Instance:** IP address of the application server**HA Score:** Normal**Auto Clear Seconds:** N/A**OID:** ipfeIpfeBackendUnderloadedNotify**Recovery:**

None required. Underloaded application servers do not impact traffic processing. This alarm will clear when traffic statistics reveal that the application server is no longer underloaded.

**5008 - Out of Balance: High****Alarm Group:** IPFE

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | Traffic statistics reveal that an application server is processing higher than average load and will not receive new connections.  |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | IP address of the overloaded application server  |
|                            | <b>Note:</b> When traffic statistics indicate that the application server is no longer overloaded, this alarm will clear.  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | N/A  |
| <b>OID:</b>                | ipfeIpfeBackendOverloadedNotify  |
| <b>Recovery:</b>           |  |
|                            | <ol style="list-style-type: none"> <li>1. The IPFE will monitor traffic statistics and will not assign connections to the overloaded application server until statistics indicate that the server is no longer overloaded.</li> <li>2. Check the status of the application servers by navigating to the <b>Status &amp; Manage &gt; Server</b> page.</li> <li>3. Consult the application server's documentation for recovery steps.</li> </ol> |

### 5009 - No available servers in target set

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | Through monitoring of the application servers, the IPFE learns that no server in a target set is available. The associated measurement, TxReject, will also show counts (refer to the <i>DSR Measurements Reference</i> 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. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | "tsa N has no available servers" where N is 1-16  |
|                            | <b>Note:</b> When at least one application server in a target set becomes available, this alarm will clear.   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | N/A   |
| <b>OID:</b>                | ipfeIpfeNoAvailableAppServersNotify   |
| <b>Recovery:</b>           |   |
|                            | <ol style="list-style-type: none"> <li>1. Ensure that application servers have been configured for the target set address by viewing <b>IPFE &gt; Configuration &gt; Target Sets</b>.</li> <li>2. Check the status of the application servers by navigating to the <b>Status &amp; Manage &gt; Server</b> page.</li> <li>3. Consult the application server's documentation for recovery steps.</li> </ol>                                     |

4. Ensure that `ipfeNetUpdate.sh` has been run by looking for the following lines in `/etc/sysconfig/network` on the IPFE blades:

```
IPV6FORWARDING=yes
IPV6_AUTOCONF=no
```

If `ipfeNetUpdate.sh` has not been run:

- Log in as **root**.
  - At the prompt, type `ipfeNetUpdate.sh`
  - At the prompt, type `init 6`
  - Repeat for each IPFE blade.
5. 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 \(MOS\)](#) for assistance.

### 5010 - Unknown Linux iptables command error

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | The IPFE received an unknown error parsing Linux iptables output. This is an internal software error. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | "error parsing iptables output"   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | N/A   |
| <b>OID:</b>                | ipfeIpfeErrorParsingIptablesOutputNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 5011 - System or platform error prohibiting operation

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | IPFE  |
| <b>Description:</b> | An internal software error.   |
| <b>Severity:</b>    | Critical  |
| <b>Instance:</b>    | Description of the problem. <ul style="list-style-type: none"> <li>• "Error opening ethernet listeners"</li> <li>• "No network cards found"</li> <li>• "Cannot update <code>/proc/irq/N/smp_affinity</code> setting"</li> <li>• "System has less than 16 CPUs"</li> </ul> <p><b>Note:</b> The IPFE detects if it has been installed on a virtual machine and will not raise this alarm.</p> |
| <b>HA Score:</b>    | 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**. The **Server Status** page appears.
  - b) Click to select the IPFE to restart.
  - c) Click **Restart**.  
 A warning message appears: **Are you sure you want to restart application software on the following server(s)? <server name>**.
  - d) Click **OK** to continue.
  - e) If the alarm still does not clear, check the Ethernet devices and CPUs.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**5012 - Signaling interface heartbeat timeout**

**Alarm Group:** IPFE  
**Description:** Heartbeats to monitor the liveness of a signaling interface have timed out.  
**Severity:** Critical  
**Instance:** The name of the Ethernet interface affected, e.g., "bond0.5", etc.  
**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.
3. Review currently active platform alarms.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**5013 - Throttling traffic**

**Alarm Group:** IPFE  
**Description:** IPFE has seen traffic in excess of Global Packet Rate Limit and is dropping packets in order to throttle the traffic.  
**Severity:** Critical  
**Instance:** The number of packets that have been throttled

|                            |                                 |
|----------------------------|---------------------------------|
| <b>HA Score:</b>           | Degraded                        |
| <b>Auto Clear Seconds:</b> | N/A                             |
| <b>OID:</b>                | ipfeIpfeThrottlingTrafficNotify |

**Recovery:**

1. Compare the setting for the Global Packet Rate Limit configuration found under **IPFE > Configuration > Options** with the system's performance specifications and determine if a higher setting is reasonable.
2. Review macro conditions that lead to high signal rate.
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**5100 - Traffic overload**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | Total IPFE signaling traffic rate is approaching or exceeding its engineered capacity.          |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | N/A   |
|                            | <b>Note:</b> If the signaling traffic declines below the clear threshold, the alarm will clear. |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | N/A   |
| <b>OID:</b>                | ipfeIpfeTrafficOverloadNotify   |

**Recovery:**

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. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**5101 - CPU Overload**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | CPU utilization is approaching maximum levels.  |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | ipfeIpfeCpuOverloadNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## 5102 - Disk Becoming Full

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | Disk space utilization is approaching maximum levels.                                   |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | ipfeIpfeDiskUsageNotify   |

### Recovery:

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## 5103 - Memory Overload

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | IPFE  |
| <b>Description:</b>        | IPFE memory utilization is approaching maximum levels.                                  |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | ipfeIpfeMemoryOverloadNotify  |

### Recovery:

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## OAM (10000-10999)

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

### 10000 - Incompatible database version

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | DB   |
| <b>Description:</b> | The database version is incompatible with the installed software database version. |

**Severity:** Critical  
**Instance:** N/A  
**HA Score:** Failed  
**Auto Clear Seconds:** 300  
**OID:** tekelecIncompatibleDatabaseVersionNotify  
**Recovery:**  
 It is recommended to contact [My Oracle Support \(MOS\)](#).

### 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:**  
 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:**  
 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:**  
 It is recommended to contact [My Oracle Support \(MOS\)](#).

#### 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:**  
 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:**  
 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**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:** awpss7TekelecProvisioningManuallyDisabledNotify

**Recovery:**

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.  
**Severity:** Critical  
**Instance:** N/A  
**HA Score:** Failed  
**Auto Clear Seconds:** This alarm does not autoclear.  
**OID:** awpss7OAGTCfgProvDbNoSyncNotify

**Recovery:**

1. Monitor the replication status using the **Status & Manage > Replication GUI** page.
2. If alarm persists for more than one hour, it is recommended to contact [My Oracle Support \(MOS\)](#).

**10010 - Stateful db from mate not yet synchronized**

**Alarm Group:** HA  
**Description:** The stateful database is not synchronized with the mate database.

|                            |                                |
|----------------------------|--------------------------------|
| <b>Severity:</b>           | Minor                          |
| <b>Instance:</b>           | N/A                            |
| <b>HA Score:</b>           | Degraded                       |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear. |
| <b>OID:</b>                | awpss7OAGTStDbNoSyncNotify     |

**Recovery:**

If alarm persists for more than 30 seconds, it is recommended to contact [My Oracle Support \(MOS\)](#).

**10011 - Cannot monitor table**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | OAM                                    |
| <b>Description:</b>        | Monitoring for table cannot be set up. |
| <b>Severity:</b>           | Major                                  |
| <b>Instance:</b>           | N/A                                    |
| <b>HA Score:</b>           | Degraded                               |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.         |
| <b>OID:</b>                | awpss7OAGTCantMonitorTableNotify       |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**10012 - Table change responder failed**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | OAM  |
| <b>Description:</b>        | The responder for a monitored table failed to respond to a table change. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Degraded   |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.   |
| <b>OID:</b>                | awpss7OAGTResponderFailedNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**10013 - Application restart in progress**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | HA                                     |
| <b>Description:</b> | An application restart is in progress. |

|                            |                                |
|----------------------------|--------------------------------|
| <b>Severity:</b>           | Minor                          |
| <b>Instance:</b>           | N/A                            |
| <b>HA Score:</b>           | Normal                         |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear. |
| <b>OID:</b>                | awpss7OAGTApplSWDisabledNotify |

**Recovery:**

If duration of alarm is greater than two seconds, it is recommended to contact [My Oracle Support \(MOS\)](#).

**10020 - Backup failure**

|                            |                                |
|----------------------------|--------------------------------|
| <b>Alarm Group:</b>        | DB                             |
| <b>Description:</b>        | Database backup failed.        |
| <b>Severity:</b>           | Minor                          |
| <b>Instance:</b>           | N/A                            |
| <b>HA Score:</b>           | Normal                         |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear. |
| <b>OID:</b>                | awpss7ApwBackupFailureNotify   |

**Recovery:**

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

**10050 - Resource Audit Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | AUD                                     |
| <b>Description:</b>        | Database backup failed.                 |
| <b>Severity:</b>           | Minor                                   |
| <b>Instance:</b>           |   |
| <b>HA Score:</b>           | Normal                                  |
| <b>Auto Clear Seconds:</b> | 0                                       |
| <b>OID:</b>                | awpss7TekelecResourceAuditFailureNotify |

**Recovery:****10051 - Route Deployment Failed**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | AUD   |
| <b>Description:</b> | An error occurred in the deployment of a network. |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | Route ID that failed to deploy  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | awpss7TekelecRouteDeploymentFailedNotify                                  |
| <b>Recovery:</b>           | Edit the route to choose a gateway that is reachable or delete the route. |

### 10052 - Route discovery failed

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | AUD   |
| <b>Description:</b>        | An error occurred in the discovery of network routes.   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | awpss7TekelecRouteDiscoveryFailedNotify   |
| <b>Recovery:</b>           | If the problem persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a> . |

### 10053 - Route deployment failed - no available device

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | AUD   |
| <b>Description:</b>        | A suitable device could not be identified for the deployment of a network route.  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | Route ID that failed to deploy  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | awpss7TekelecNoRouteDeviceNotify  |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. Deploy the route on a specific device instead of using the "AUTO" device.</li> <li>2. Ensure that every server in the server group has a usable device for the selected gateway.</li> </ol> |

### 10054 - Device deployment failed

|                     |     |
|---------------------|-----|
| <b>Alarm Group:</b> | AUD |
|---------------------|-----|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | An error occurred in the deployment of a network device. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | Device name that failed to deploy                        |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0  |
| <b>OID:</b>                | awpss7TekelecDeviceDeploymentFailedNotify                |
| <b>Recovery:</b>           | Edit or delete the device.                               |

### 10055 - Device discovery failed

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | AUD   |
| <b>Description:</b>        | An error occurred in the discovery of network devices.  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | awpss7TekelecDeviceDiscoveryFailedNotify  |
| <b>Recovery:</b>           | If the problem persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a> . |

### 10073 - Server Group Max Allowed HA Role Warning

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | The server group has received the maximum number of allowed HA role warnings. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | Affected Server Group name  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | awpss7OAGTSgMaxAllowedHARoleWarnNotify  |

**Recovery:**

1. Login to the SO GUI and navigate to the HA page (**Main Menu > 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, login to the server (**Main Menu > Status & Manage > Server**).
4. Click on the Active server and press the **Restart** button 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 the following command:

```
# ha.mystate
```

### 10074 - Standby server degraded while mate server stabilizes

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | HA   |
| <b>Description:</b>        | The standby server has temporarily degraded while the new active server stabilizes following a switch of activity. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Degraded   |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.   |
| <b>OID:</b>                | awpss7HASbyRecoveryInProgressNotify  |

**Recovery:**

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

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | HA   |
| <b>Description:</b>        | The server is no longer providing services because application processes have been manually stopped. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.   |
| <b>OID:</b>                | awpss7HAMtceStopApplicationsNotify   |

**Recovery:**

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

|                    |    |
|--------------------|----|
| <b>Event Type:</b> | HA |
|--------------------|----|

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | The Applications on the Standby server have not been restarted after an active-to- standby transition since h_FailureCleanupMode is set to 0. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 1   |
| <b>OID:</b>              | awpss7FailureRecoveryWithoutAppRestartNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**10100 - Log export started**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | LOG                                     |
| <b>Description:</b>      | Log files export operation has started. |
| <b>Severity:</b>         | Info                                    |
| <b>Instance:</b>         | N/A                                     |
| <b>HA Score:</b>         | Normal                                  |
| <b>Throttle Seconds:</b> | 1                                       |
| <b>OID:</b>              | awpss7TekelecLogExportStartNotify       |

**Recovery:**

No action required.

**10101 - Log export successful**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG  |
| <b>Description:</b>      | The log files export operation completed successfully. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | N/A  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | awpss7TekelecLogExportSuccessNotify                    |

**Recovery:**

No action required.

**10102 - Log export failed**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG                                    |
| <b>Description:</b>      | The log files export operation failed. |
| <b>Severity:</b>         | Info                                   |
| <b>Instance:</b>         | N/A                                    |
| <b>HA Score:</b>         | Normal                                 |
| <b>Throttle Seconds:</b> | 1                                      |
| <b>OID:</b>              | awpss7TekelecLogExportFailedNotify     |

**Recovery:**

1. Verify the export request and try the export again.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**10103 - Log export already in progress**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | LOG   |
| <b>Description:</b>      | Log files export operation not run - export can only run on Active Network OAMP server. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 1   |
| <b>OID:</b>              | awpss7TekelecLogExportNotRunNotify  |

**Recovery:**

Restart export operation after existing export completes.

**10104 - Log export file transfer failed**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG  |
| <b>Description:</b>      | The performance data export remote copy operation failed.  |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <Task ID>  |
|                          | <b>Note:</b> <Task ID> refers to the ID column found in <b>Main Menu &gt; Status &amp; Manage &gt; Tasks &gt; Active Tasks</b> . |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | awpss7TekelecExportXferFailedNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**10105 - Log export cancelled - user request**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG  |
| <b>Description:</b>      | The log files export operation cancelled by user.  |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <Task ID>  |
|                          | <b>Note:</b> <Task ID> refers to the ID column found in <b>Main Menu &gt; Status &amp; Manage &gt; Tasks &gt; Active Tasks</b> . |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | awpss7TekelecLogExportCancelledUserNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**10106 - Log export cancelled - duplicate request**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG  |
| <b>Description:</b>      | The log files export operation was cancelled because a scheduled export is queued already.                                       |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <Task ID>  |
|                          | <b>Note:</b> <Task ID> refers to the ID column found in <b>Main Menu &gt; Status &amp; Manage &gt; Tasks &gt; Active Tasks</b> . |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | awpss7TekelecLogExportCancelledDuplicateNotify   |

**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 \(MOS\)](#) for assistance.

**10107 - Log export cancelled - queue full**

|                    |     |
|--------------------|-----|
| <b>Event Type:</b> | LOG |
|--------------------|-----|

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | The log files export operation cancelled because the export queue is full.  |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <Task ID><br><b>Note:</b> <Task ID> refers to the ID column found in <b>Main Menu &gt; Status &amp; Manage &gt; Tasks &gt; Active Tasks</b> .   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 1   |
| <b>OID:</b>              | awpss7TekelecLogExportCancelledQueueNotify  |
| <b>Recovery:</b>         | <ol style="list-style-type: none"> <li>1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.</li> <li>2. If the problem persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a> for assistance.</li> </ol> |

### 10108 - Duplicate scheduled log export task

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | LOG   |
| <b>Description:</b>        | A duplicate scheduled log export task has been queued.  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <Target ID><br><b>Note:</b> <Target ID> refers to the scheduled task ID found by running a report from <b>Main Menu &gt; Status &amp; Manage &gt; Tasks &gt; Scheduled Tasks</b> .  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.  |
| <b>OID:</b>                | awpss7TekelecLogExportDupSchedTaskNotify  |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.</li> <li>2. If the problem persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a> for assistance.</li> </ol> |

### 10109 - Log export queue is full

|                     |                              |
|---------------------|------------------------------|
| <b>Alarm Group:</b> | LOG                          |
| <b>Description:</b> | The log export queue is full |
| <b>Severity:</b>    | 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 **Main Menu > Status & Manage > Tasks > Active Tasks** or **Main Menu > Status & Manage > Tasks > Scheduled Tasks**.

**HA Score:** Normal

**Auto Clear Seconds:** This alarm does not autoclear.

**OID:** awpss7TekelecLogExportQueueFullNotify

**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 \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**10112 - Certificate Cannot Be Used**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | AUD  |
| <b>Description:</b>        | The certificate cannot be used because the certificate is not available yet. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <CertificateName>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | certificateCannotBeUsed  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**10115 - Health Check Started**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | LOG                                     |
| <b>Description:</b>      | Upgrade health check operation started. |
| <b>Severity:</b>         | Info                                    |
| <b>Instance:</b>         | <ServerGroupName>                       |
| <b>HA Score:</b>         | Normal                                  |
| <b>Throttle Seconds:</b> | N/A                                     |
| <b>OID:</b>              | tekelecLogHealthCheckStart              |

**Recovery:**

No action required.

**10116 - Health Check Successful**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG  |
| <b>Description:</b>      | Upgrade health check operation completed successfully. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ServerGroupName>                                      |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | N/A  |
| <b>OID:</b>              | tekelecLogHealthCheckSuccess                           |

**Recovery:**

No action required.

**10117 - Health Check Failed**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG                                    |
| <b>Description:</b>      | Upgrade health check operation failed. |
| <b>Severity:</b>         | Info                                   |
| <b>Instance:</b>         | <ServerGroupName>                      |
| <b>HA Score:</b>         | Normal                                 |
| <b>Throttle Seconds:</b> | N/A                                    |
| <b>OID:</b>              | tekelecLogHealthCheckFailed            |
| <b>Recovery:</b>         | No action required.                    |

**10118 - Health Check Not Run**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | LOG  |
| <b>Description:</b>      | Upgrade health check not run.  |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ServerGroupName>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | N/A  |
| <b>OID:</b>              | tekelecLogHealthCheckNotRun  |
| <b>Recovery:</b>         | It is recommended to contact <a href="#">My Oracle Support (MOS)</a> . |

**10120 - Server Group Upgrade Started**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | LOG   |
| <b>Description:</b>      | The server group upgrade operation has started. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <ServerGroupName>                               |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 1   |
| <b>OID:</b>              | tekelecLogSgUpgradeStart                        |
| <b>Recovery:</b>         | No action required.                             |

**10121 - Server Group Upgrade Cancelled - Validation Failed**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | The server group upgrade operation has been cancelled due to validation failure. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ServerGroupName>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | tekelecLogSgUpgradeCancelled   |
| <b>Recovery:</b>         | No action required.  |

**10122 - Server Group Upgrade Successful**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | The server group upgrade operation completed successfully. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ServerGroupName>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | tekelecLogSgUpgradeSuccess                                 |
| <b>Recovery:</b>         | No action required.  |

**10123 - Server Group Upgrade Failed**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | The server group upgrade operation failed. |
| <b>Severity:</b>         | Info                                       |
| <b>Instance:</b>         | <ServerGroupName>                          |
| <b>HA Score:</b>         | Normal                                     |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | tekelecLogSgUpgradeFailed                  |
| <b>Recovery:</b>         | No action required.                        |

**10124 - Server Group Upgrade Cancelled - User Request**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | The user cancelled the server group upgrade operation. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ServerGroupName>                                      |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | tekelecLogSgUpgradeCancelledUser                       |
| <b>Recovery:</b>         | No action required.                                    |

**10130 - Server Upgrade Started**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | LOG                                       |
| <b>Description:</b>      | The server upgrade operation has started. |
| <b>Severity:</b>         | Info                                      |
| <b>Instance:</b>         | <HostName>                                |
| <b>HA Score:</b>         | Normal                                    |
| <b>Throttle Seconds:</b> | 1   |
| <b>OID:</b>              | tekelecLogServerUpgradeStart              |
| <b>Recovery:</b>         | No action required.                       |

**10131 - Server Upgrade Cancelled**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | The server upgrade operation has been cancelled due to validation failure. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <HostName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | tekelecLogServerUpgradeCancelled   |
| <b>Recovery:</b>         | No action required.  |

**10132 - Server Upgrade Successful**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | The server upgrade operation completed successfully. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <HostName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | tekelecLogServerUpgradeSuccess                       |
| <b>Recovery:</b>         | No action required.                                  |

**10133 - Server Upgrade Failed**

|                          |                                      |
|--------------------------|--------------------------------------|
| <b>Event Group:</b>      | LOG                                  |
| <b>Description:</b>      | The server upgrade operation failed. |
| <b>Severity:</b>         | Info                                 |
| <b>Instance:</b>         | <HostName>                           |
| <b>HA Score:</b>         | Normal                               |
| <b>Throttle Seconds:</b> | 1                                    |
| <b>OID:</b>              | tekelecLogServerUpgradeFailed        |
| <b>Recovery:</b>         | No action required.                  |

**10134 - Server Upgrade Failed**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | LOG  |
| <b>Description:</b>        | The server upgrade operation failed.   |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <HostName>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0  |
| <b>OID:</b>                | tekelecLogServerUpgradeFailAlm   |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. If there are servers in the server group that have successfully upgraded, you will need to individually restart the upgrade on that server. Navigate to the Upgrade page (<b>Administration &gt; Software Management &gt; Upgrade</b>).</li> </ol> |

2. Select the "Server Group" tab containing the server that raised the alarm.
3. Select the individual server(s) and then click the **Server Upgrade** button to start the upgrade on those 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.
4. If no servers in the group have been upgraded, you can select **Auto Upgrade** to upgrade all servers in the server group. If a server upgrade has failed already, the alarm will be cleared when the server begins to upgrade.  
  
**Note:** The active server in the NO server group will never upgrade automatically.

### 10140 - Site Upgrade Started

|                          |                                 |
|--------------------------|---------------------------------|
| <b>Event Type:</b>       | LOG                             |
| <b>Description:</b>      | Site upgrade operation started. |
| <b>Severity:</b>         | Info                            |
| <b>Instance:</b>         | Site name                       |
| <b>HA Score:</b>         | Normal                          |
| <b>Throttle Seconds:</b> | N/A                             |
| <b>OID:</b>              | tekelecLogSiteUpgradeStart      |
| <b>Recovery:</b>         | No action required.             |

### 10141 - Site Upgrade Cancelled

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | LOG   |
| <b>Description:</b>      | Site upgrade cancelled - validation failed. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Site name                                   |
| <b>HA Score:</b>         | Normal                                      |
| <b>Throttle Seconds:</b> | N/A   |
| <b>OID:</b>              | tekelecLogSiteUpgradeCancelled              |
| <b>Recovery:</b>         | No action required.                         |

### 10142 - Site Upgrade Successful

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | LOG  |
| <b>Description:</b> | Site upgrade operation completed successfully. |

**Severity:** Info  
**Instance:** Site name  
**HA Score:** Normal  
**Throttle Seconds:** N/A  
**OID:** tekelecLogSiteUpgradeSuccess  
**Recovery:**  
 No action required.

### 10143 - Site Upgrade Failed

**Event Type:** LOG  
**Description:** Site upgrade operation failed.  
**Severity:** Info  
**Instance:** Site name  
**HA Score:** Normal  
**Throttle Seconds:** N/A  
**OID:** tekelecLogSiteUpgradeFailed  
**Recovery:**  
 No action required.

### 10144 - Site Upgrade Cancelled - User Request

**Event Type:** LOG  
**Description:** Site upgrade cancelled by user.  
**Severity:** Info  
**Instance:** Site name  
**HA Score:** Normal  
**Throttle Seconds:** N/A  
**OID:** tekelecLogSiteUpgradeCancelledUser  
**Recovery:**  
 No action required.

### 10151 - Login successful

**Event Type:** LOG  
**Description:** The login operation was successful.  
**Severity:** Info

**Instance:** N/A  
**HA Score:** Normal  
**Throttle Seconds:** 1  
**OID:** awpss7TekelecLoginSuccessNotify  
**Recovery:**  
 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:** awpss7TekelecLoginFailedNotify  
**Recovery:**  
 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:** awpss7TekelecLogoutSuccessNotify  
**Recovery:**  
 No action required.

### 10154 - User Account Disabled

**Alarm Group:** AUTH  
**Description:** User account has been disabled due to multiple login failures.  
**Severity:** Minor

|                            |                                    |
|----------------------------|------------------------------------|
| <b>Instance:</b>           | N/A                                |
| <b>HA Score:</b>           | Normal                             |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.     |
| <b>OID:</b>                | awpss7TekelecAccountDisabledNotify |

**Recovery:**

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

**10155 - SAML Login Successful**

|                          |                                     |
|--------------------------|-------------------------------------|
| <b>Event Group:</b>      | LOG                                 |
| <b>Description:</b>      | SAML Login Successful               |
| <b>Severity:</b>         | Info                                |
| <b>Instance:</b>         | N/A                                 |
| <b>HA Score:</b>         | Normal                              |
| <b>Throttle Seconds:</b> | 1                                   |
| <b>OID:</b>              | awpss7TekelecSamlLoginSuccessNotify |

**Recovery:**

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**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | LOG  |
| <b>Description:</b>      | An attempt to login to the GUI via conventional login or via SSO login failed. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | N/A  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | 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 \(MOS\)](#) if the problem persists.

**10200 - Remote database reinitialization in progress**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | CFG   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <hostname of remote server>   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.  |
| <b>OID:</b>                | awpss7ApwSgDbReinitNotify   |

**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 \(MOS\)](#).

**10300 - SNMP Trapping Not Configured**

|                           |                                       |
|---------------------------|---------------------------------------|
| <b>Alarm Group</b>        | DB                                    |
| <b>Description</b>        | SNMP Trapping Not Configured for Site |
| <b>Severity</b>           | Minor                                 |
| <b>Instance</b>           | <Hostname>                            |
| <b>HA Score</b>           | Normal                                |
| <b>Auto Clear Seconds</b> | 0 (zero)                              |
| <b>OID</b>                | apwSnmptTrappingNotConfiguredForSite  |

**Recovery**

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

**IDIH (11500-11549)**

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

**11500 - Tracing Suspended**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | IDIH   |
| <b>Description:</b>        | IDIH trace has been suspended due to DA-MP (danger of) CPU congestion. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterTracingSuspendedAlarmNotify                             |

**Recovery:**

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

**11501 - Trace Throttling Active**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | IDIH   |
| <b>Description:</b>        | Troubleshooting trace has been throttled on some DA-MPs due to IDIH TTR bandwidth usage exceeding provisioned limit. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterTracingThrottledAlarmNotify   |

**Recovery:**

No action required

**11502 - Troubleshooting Trace Started**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | IDIH  |
| <b>Description:</b>      | A troubleshooting trace instance was started. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TraceInstanceId>                             |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0   |
| <b>OID:</b>              | eagleXgDiameterIDIHTraceStartedNotify         |

**Recovery:**

No action required.

### 11503 - Troubleshooting Trace Stopped

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | IDIH  |
| <b>Description:</b>      | A troubleshooting trace instance was stopped. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TraceInstanceId>                             |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0   |
| <b>OID:</b>              | eagleXgDiameterIDIHTraceStoppedNotify         |
| <b>Recovery:</b>         | No action required                            |

### 11506 - Invalid IDIH-Trace AVP

|                          |   |
|--------------------------|---|
| <b>Alarm Group:</b>      | IDIH  |
| <b>Description:</b>      | An IDIH-Trace AVP has been received with an invalid format. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransConnName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | eagleXgDiameterInvalidIDIHTraceAvpNotify                    |
| <b>Recovery:</b>         |   |

1. If the message came from a peer that is not a DA-MP, verify that 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 \(MOS\)](#).

### 11507 - Unable to run network trace at this site

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | IDIH   |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <TraceName>  |

**HA Score:** Normal  
**Throttle Seconds:** 0  
**OID:** eagleXgDiameterUnableToRunNetworkTraceAtThisSiteNotify

**Recovery:**

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:**

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:**

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.

|                                   |  |
|-----------------------------------|--|
| <b>Severity:</b>                  | Minor  |
| <b>Instance&lt;TraceName&gt;:</b> |  |
| <b>HA Score:</b>                  | Normal   |
| <b>Auto Clear Seconds:</b>        | 0 (zero)   |
| <b>OID:</b>                       | eagleXgDiameterNetworkTraceActivationErrorNotify |
| <b>Recovery:</b>                  | No action required.                              |

### 11511 - Invalid DIH HostName

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | Unable to connect via ComAgent to remote DIH server with hostname. |
| <b>Severity</b>           | Minor  |
| <b>Instance</b>           | String of Configured DIH HostName                                  |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0  |
| <b>OID</b>                | eagleXgDiameterInvalidDihHostNameAlarmNotify                       |
| <b>Recovery</b>           | No action required.  |

### SS7/Sigtran Alarms (19200-19299)

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

#### 19200 - RSP/Destination unavailable

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7  |
| <b>Description:</b>        | Unable to access the SS7 Destination Point Code because the RSP status is Unavailable. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | RSP Name   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.   |
| <b>OID:</b>                | awpss7M3r1RspUnavailableNotify   |

**Recovery:**

1. RSP/Destination status can be monitored from the SOAM GUI **SS7/Sigtran > Maintenance > Remote Signaling Points**.
  - If the RSP/Destination becomes Unavailable due to a link set failure, the MP server will attempt to automatically recover all links not manually disabled.
  - If the RSP/Destination 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 that the adjacent server is not under maintenance.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**19201 - RSP/Destination route unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SS7   |
| <b>Description:</b>        | Unable to access the SS7 Destination point code via this route. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <Route Name>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.                                  |
| <b>OID:</b>                | awpss7M3r1RouteUnavailableNotify                                |

**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 that the adjacent server is not under maintenance.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**19202 - Linkset unavailable**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | SS7   |
| <b>Description:</b> | The SS7 link set to an adjacent signaling point has failed. |
| <b>Severity:</b>    | Major   |
| <b>Instance:</b>    | <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 \(MOS\)](#).

**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 \(MOS\)](#).

**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 \(MOS\)](#).

**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:**

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

### 19207 - TFR received

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | TFR message received by M3RL layer; an adjacent point code has reported that an available route to the RSP/Destination has a restriction/limitation. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | N/A  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | 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

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | TFC message received by M3RL layer; an adjacent or non-adjacent point code is reporting the congestion level of a RSP/Destination. |
| <b>Severity:</b>         | Info   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 30   |
| <b>Instance:</b>         | N/A  |
| <b>OID:</b>              | 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

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | SS7   |
| <b>Description:</b> | A message was discarded due to a routing error. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | N/A   |

|                          |                                |
|--------------------------|--------------------------------|
| <b>HA Score:</b>         | Normal                         |
| <b>Throttle Seconds:</b> | 10                             |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance.

**19210 - M3RL routing error - invalid NI**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | SS7  |
| <b>Description:</b> | <p>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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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:           <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> </li> </ul> <p>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.</p> |
| <b>Severity:</b>    | 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 the GUI main menu under **SS7/Sigtran > Configuration > Remote Signaling Points**.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**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 \(MOS\)](#).

**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. Select **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. View the active alarms and event history logs by selecting **Alarms & Events > View Active** and **Alarms & Events > View History**. Look for significant events that may affect the IP network, associations, or links.
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 19226 - Timedout waiting for ASP-UP-ACK

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | When an association is in the <b>Enabled</b> 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 <b>Blocked</b> or <b>Disabled</b> , or the SCTP transport fails, or the ASP-UP-ACK is received. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <AssocName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | awpss7TimedOutWaitingForAspUpAckNotify  |

#### Recovery:

1. Verify that the adjacent server on the Signaling Gateway is not under maintenance.
2. Verify that 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 \(MOS\)](#).

### 19227 - Received unsolicited ASP-DOWN-ACK

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | SS7  |
| <b>Description:</b> | 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 <b>Enabled</b> , the MP server will automatically attempt to bring the association back to ASP-UP. This is done by sending an ASP-UP. The MP server will continue to send ASP-UP until an ASP-UP-ACK is received, the SCTP association comes down, or the association administrative state is changed to <b>Blocked</b> or <b>Disabled</b> . |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <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 \(MOS\)](#).

**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 that the adjacent server on the Signaling Gateway is not under maintenance.
2. Verify that 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 \(MOS\)](#).

**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 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 \(MOS\)](#).

**19231 - Received invalid M3UA message**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | The far-end has sent an invalid M3UA message to which the MP server has responded with an M3UA ERROR message.                                       |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <LinkName> or <AssocName> Information about the type of error and the accompanying diagnostic data is included in the event additional information. |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | awpss7ReceivedInvalidM3uaMessageNotify  |

**Recovery:**

- Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the malformed message.
  - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
  - Error code 0x03 indicates an unsupported M3UA message class.
  - Error code 0x04 indicates an unsupported M3UA message type.
  - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
  - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
  - Error code 0x12 indicates a parameter field error. Parameter is malformed (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.
- If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**19233 - Failed to send non-DATA message**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | SS7  |
| <b>Description:</b> | 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: <ul style="list-style-type: none"> <li>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.</li> </ul> |

- 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 \(MOS\)](#).

### 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 \(MOS\)](#).

### 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 \(MOS\)](#).

## 19240 - Remote SCCP subsystem prohibited

**Alarm Group:** SS7

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

**Severity:** Minor

**Instance:** <RMU>

|                            |   |
|----------------------------|---|
| <b>HA Score:</b>           | Normal                                    |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.            |
| <b>OID:</b>                | 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 that 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 \(MOS\)](#).

**19241 - SCCP malformed or unsupported message**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | 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 \(MOS\)](#).

### 19242 - SCCP Hop counter violation

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | SCCP discarded an ingress message because a Hop Counter violation was detected. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | 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 \(MOS\)](#).

### 19243 - SCCP routing failure

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | N/A  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | 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

- If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 19244 - SCCP routing failure network status

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | awpss7SccpRoutingFailureNetworkStatusNotify   |

#### Recovery:

- 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**.
- Verify that IP network connectivity exists between the MP server and the adjacent servers.
- Check the event history logs for additional SS7 events or alarms from this MP server.
- Verify that the adjacent server is not under maintenance.
- If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 19245 - SCCP GTT failure

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | SCCP Global Title Translation has failed to determine a destination for a PDU. SCCP is invoking the message return procedure. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | awpss7SccpGttFailureNotify  |

#### Recovery:

- 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 \(MOS\)](#).

## 19246 - Local SCCP subsystem prohibited

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7  |
| <b>Description:</b>        | The status of the local SCCP subsystem has changed to <b>Prohibited</b> . This alarm is raised for one of the following conditions: <ul style="list-style-type: none"> <li>• When a new local SSN is configured and is in the disabled state.</li> <li>• When a GUI maintenance operation is performed to disable the state of the local SSN.</li> <li>• On a system restart where the local SSN was in disabled state prior to the system restart.</li> </ul> |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <LSP>, <SSN>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.   |
| <b>OID:</b>                | awpss7SCCPLocalSubsystemProhibitedNotify   |

### Recovery:

To clear the alarm:

- a) On the SOAM GUI main menu, 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

|                          |                                     |
|--------------------------|-------------------------------------|
| <b>Event Type:</b>       | SS7                                 |
| <b>Description:</b>      | SCCP Segmentation Procedure Failure |
| <b>Severity:</b>         | Info                                |
| <b>Instance:</b>         | N/A                                 |
| <b>HA Score:</b>         | Normal                              |
| <b>Throttle Seconds:</b> | 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 the [My Oracle Support \(MOS\)](#) 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 the [My Oracle Support \(MOS\)](#) 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 the GUI main menu under **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 \(MOS\)](#).

**19251 - Ingress message rate**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SS7   |
| <b>Description:</b>        | The ingress message rate (messages per second) for the MP is approaching or exceeding its engineered traffic handling capacity. |
| <b>Severity:</b>           | Minor, Major, Critical as shown in the GUI under <b>Alarms &amp; Events &gt; View Active</b> .                                  |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.  |
| <b>OID:</b>                | 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 the GUI main menu under **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 \(MOS\)](#).

**19252 - PDU buffer pool utilization**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | SS7  |
| <b>Description:</b> | 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. |

|                            |  |
|----------------------------|--|
| <b>Severity:</b>           | Minor, Major, Critical as shown in the GUI under <b>Alarms &amp; Events &gt; View Active</b> . |
| <b>Instance:</b>           | <PoolName> Values: ANSI, ITUI, ITUN  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.   |
| <b>OID:</b>                | 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 the GUI main menu under **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 \(MOS\)](#).

**19253 - SCCP stack event queue utilization**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SS7   |
| <b>Description:</b>        | The percent utilization of the MP's SCCP stack event queue is approaching its maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical as shown in the GUI under <b>Alarms &amp; Events &gt; View Active</b> .  |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.  |
| <b>OID:</b>                | 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 the GUI main menu under **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 \(MOS\)](#).

### 19254 - M3RL stack event queue utilization

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SS7   |
| <b>Description:</b>        | The percent utilization of the MP's M3RL Stack Event Queue is approaching its maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical as shown in the GUI under <b>Alarms &amp; Events &gt; View Active</b> .  |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.  |
| <b>OID:</b>                | 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 the GUI main menu under **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 \(MOS\)](#).

### 19255 - M3RL network management event queue utilization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7  |
| <b>Description:</b>        | The percent utilization of the MP's M3RL Network Management Event Queue is approaching its maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical as shown in the GUI under <b>Alarms &amp; Events &gt; View Active</b> .               |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 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 the GUI main menu under **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 \(MOS\)](#).

### 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 the GUI main menu under **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 \(MOS\)](#).

**19258 - SCTP Aggregate Egress queue utilization**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SS7   |
| <b>Description:</b>        | The percent utilization of events queued to all SCTP associations on the MP server is approaching maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical as shown in the GUI under <b>Alarms &amp; Events &gt; View Active</b> .                      |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | This alarm does not autoclear.  |
| <b>OID:</b>                | 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 the GUI main menu under **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 \(MOS\)](#).

**19259 - Operation discarded due to local resource limitation**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | Operation discarded due to local resource limitation |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | Application name                                     |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

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

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | Transaction could not be delivered to remote TCAP peer due to conditions in the network. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | Application name   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

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

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | Operation discarded due to malformed component received from remote TCAP peer |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Application name  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

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

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | Transaction discarded due to malformed dialogue message received from local TC User |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Application name  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | awpss7TcapMalformedDialogueFromLocalNotify  |

**Recovery:**

1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

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

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | Transaction discarded due to malformed dialogue message received from local TC User |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Application name  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | awpss7TcapMalformedDialogueFromRemoteNotify   |

**Recovery:**

1. This event indicates that 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 \(MOS\)](#) for assistance if needed.

### 19265 - Unexpected event received from local TC User

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | SS7   |
| <b>Description:</b> | Unexpected event received from local TC User. |
| <b>Severity:</b>    | Info  |

|                          |  |
|--------------------------|--|
| <b>Instance:</b>         | Application name                       |
| <b>HA Score:</b>         | Normal                                 |
| <b>Throttle Seconds:</b> | 30                                     |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

**19266 - Unexpected event received from remote TCAP peer**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | SS7   |
| <b>Description:</b>      | Unexpected event received from remote TCAP peer |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Application name                                |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

**19267 - Dialogue removed by dialogue cleanup timer**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | Dialogue removed by dialogue cleanup timer |
| <b>Severity:</b>         | Info                                       |
| <b>Instance:</b>         | Application name                           |
| <b>HA Score:</b>         | Normal                                     |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

**19268 - Operation removed by invocation timer expiry**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | Operation removed by invocation timer expiry |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | Application name                             |
| <b>HA Score:</b>         | Normal                                       |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

### 19269 - Dialogue aborted by remote TCAP peer

|                          |                                       |
|--------------------------|---------------------------------------|
| <b>Event Type:</b>       | SS7                                   |
| <b>Description:</b>      | Dialogue aborted by remote TCAP peer  |
| <b>Severity:</b>         | Info                                  |
| <b>Instance:</b>         | Application name                      |
| <b>HA Score:</b>         | Normal                                |
| <b>Throttle Seconds:</b> | 30                                    |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

### 19270 - Received unsupported TCAP message

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7                                    |
| <b>Description:</b>      | Received unsupported TCAP message      |
| <b>Severity:</b>         | Info                                   |
| <b>Instance:</b>         | Application name                       |
| <b>HA Score:</b>         | Normal                                 |
| <b>Throttle Seconds:</b> | 30                                     |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

**19271 - Operation rejected by remote TCAP peer**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7                                    |
| <b>Description:</b>      | Operation rejected by remote TCAP peer |
| <b>Severity:</b>         | Info                                   |
| <b>Instance:</b>         | Application name                       |
| <b>HA Score:</b>         | Normal                                 |
| <b>Throttle Seconds:</b> | 30                                     |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

**19272 - TCAP active dialogue utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7                                    |
| <b>Description:</b>        | TCAP active dialogue utilization       |
| <b>Severity:</b>           | Minor, Major, Critical                 |
| <b>Instance:</b>           | Application name                       |
| <b>HA Score:</b>           | Normal                                 |
| <b>Auto Clear Seconds:</b> | 0 (alarm does not clear automatically) |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance if needed.

**19273 - TCAP active operation utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7                                    |
| <b>Description:</b>        | TCAP active operation utilization      |
| <b>Severity:</b>           | Minor, Major, Critical                 |
| <b>Instance:</b>           | Application name                       |
| <b>HA Score:</b>           | Normal                                 |
| <b>Auto Clear Seconds:</b> | 0 (alarm does not clear automatically) |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance if needed.

**19274 - TCAP stack event queue utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7                                    |
| <b>Description:</b>        | TCAP stack event queue utilization     |
| <b>Severity:</b>           | Minor, Major, Critical                 |
| <b>Instance:</b>           | Application name                       |
| <b>HA Score:</b>           | Normal                                 |
| <b>Auto Clear Seconds:</b> | 0 (alarm does not clear automatically) |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance if needed.

### 19275 - Return error from remote TCAP peer

|                          |                                       |
|--------------------------|---------------------------------------|
| <b>Event Type:</b>       | SS7                                   |
| <b>Description:</b>      | Return error from remote TCAP peer    |
| <b>Severity:</b>         | Info                                  |
| <b>Instance:</b>         | Application name                      |
| <b>HA Score:</b>         | Normal                                |
| <b>Throttle Seconds:</b> | 30                                    |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

### 19276 - SCCP Egress Message Rate

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SS7  |
| <b>Description:</b>        | The SCCP Egress Message Rate (Message per second) for the MP is approaching or exceeding its engineered traffic handling capacity. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (alarm does not clear automatically)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance if needed.

## 19281 - TCAP Routing Failure

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | SS7  |
| <b>Description:</b>      | TCAP was unable to route message due to transient conditions such as destination failure or destination unavailability |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | Hostname   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 \(MOS\)](#) 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

|                            |                                |
|----------------------------|--------------------------------|
| <b>Alarm Group:</b>        | TMF                            |
| <b>Description:</b>        | Transport Down                 |
| <b>Severity:</b>           | Major                          |
| <b>Instance:</b>           | <TransportName>                |
| <b>HA Score:</b>           | Normal                         |
| <b>Auto Clear Seconds:</b> | 0 (zero)                       |
| <b>OID:</b>                | awptransmgrTransportDownNotify |

### Recovery:

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

Additional Information for the alarm can be found in **Main Menu > 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 **Main Menu > 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 **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 \(MOS\)](#).

## 19401 - Failed to configure Transport

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | TMF   |
| <b>Description:</b>      | Failed to configure Transport               |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransportName>                             |
| <b>HA Score:</b>         | Normal                                      |
| <b>Throttle Seconds:</b> | 0 (zero)                                    |
| <b>OID:</b>              | awptransmgrFailedToConfigureTransportNotify |
| <b>Recovery:</b>         |   |

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 \(MOS\)](#) for assistance.

### 19402 - Failed to connect Transport

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | TMF                                       |
| <b>Description:</b>      | Failed to connect Transport               |
| <b>Severity:</b>         | Info                                      |
| <b>Instance:</b>         | <TransportName>                           |
| <b>HA Score:</b>         | Normal                                    |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | 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 **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 \(MOS\)](#).

### 19403 - Received malformed SCTP message (invalid length)

|                          |  |
|--------------------------|--|
| <b>Alarm Group:</b>      | TMF  |
| <b>Description:</b>      | Received malformed SCTP message (invalid length) |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <TransportName>                                  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 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 \(MOS\)](#).

### 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 \(MOS\)](#).

### 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 functioning 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 \(MOS\)](#).

### 19406 - Local Transport maintenance state change

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | TMF   |
| <b>Description:</b>      | Local Transport maintenance state change              |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransportName>                                       |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |
| <b>OID:</b>              | 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 \(MOS\)](#).

### 19407 - Failed to send Transport DATA Message

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | TMF  |
| <b>Description:</b> | Failed to send Transport DATA Message                    |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <TransportName>, <TransportAdapter>, <TransportProtocol> |
| <b>HA Score:</b>    | 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 \(MOS\)](#).

**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 from the network.
- The SCTP Association Writer process may be experiencing a problem preventing it from processing events from its event queue. The alarm log should be examined from **Main Menu > Alarms & Events**.
- If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining Mps in the server site. MP server status can be monitored from **Main Menu > Status & Control > 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 & Control > 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 \(MOS\)](#).

### 19409 - Message Rejected by ACL Filtering

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | TMF   |
| <b>Description:</b>      | The message is rejected based on configured Access Control List for Transport |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransportName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 \(MOS\)](#).

### 19410 - Adjacent Node IP Address state change

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | TMF   |
| <b>Description:</b>      | State change of an IP Address of a multihomed Adjacent Node in SCTP Transport |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransportName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |
| <b>OID:</b>              | 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 \(MOS\)](#).

**19411 - SCTP Transport closed due to failure of multihoming validation**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | TMF  |
| <b>Description:</b>      | SCTP Transport closed due to failure of multihoming validation |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <TransportName>, <TransportId>                                 |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 0 (zero)   |
| <b>OID:</b>              | 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 \(MOS\)](#).

**19412 - SCTP Transport configuration mismatched for Adjacent Node IP**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | TMF   |
| <b>Description:</b>      | IP address advertised by an Adjacent Node in INIT/INIT-ACK chunk are different from configured IP Addresses |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransportName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |
| <b>OID:</b>              | 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 \(MOS\)](#).

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

|                          |   |
|--------------------------|---|
| <b>Alarm Group:</b>      | TMF   |
| <b>Description:</b>      | SCTP Transport closed due to unsupported add/delete peer IP Address event recieved in Peer Address Notification |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransportName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 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 \(MOS\)](#).

## 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

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | SMS  |
| <b>Description</b>        | The BDF work queue depth size has reached full capacity. |
| <b>Severity</b>           | Minor  |
| <b>Instance</b>           | N/A  |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | cAFBDFQFullNotify  |

**Recovery:**

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 \(MOS\)](#) for assistance if needed.

### 19421 - BDFThrotl

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | SMS  |
| <b>Description</b>        | The BDF subsystem is throttling traffic at sender. |
| <b>Severity</b>           | Minor  |
| <b>Instance</b>           | N/A  |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | cAFBDFThrotlNotify                                 |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

**19422 - BDFInvalidPkt**

|                         |  |
|-------------------------|--|
| <b>Alarm Group</b>      | SMS  |
| <b>Description</b>      | The BDF subsystem received a StackEvent that was somehow invalid, corrupt, or could not be delivered to the application. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Source IP>  |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 0 (zero)   |
| <b>OID</b>              | cAFBroadcastDataFrameworkInvalidStackEventNotify   |

**Recovery:**

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 \(MOS\)](#) for assistance if needed.

**19800 - Communication Agent Connection Down**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | CAF   |
| <b>Description:</b>        | This alarm indicates that a Communication Agent is unable to establish transport connections with one or more other servers, and this may indicate that applications on the local server are unable to communicate with all of their peers. Generally this alarm is asserted when a server or the IP network is undergoing maintenance or when a connection has been manually disabled. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | cAFConnectionDownNotify   |

**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 connection is manually disabled, then no further action is necessary.
5. Verify that the remote server is not under maintenance.
6. Verify that IP network connectivity exists between the two connection end-points.
7. Verify that the connection's local IP address and port number are configured on remote Node.
8. Verify that the Application Process using Communication Agent plug-in is running on both ends.
9. Verify that the connection's remote IP address and port correctly identify remote's listening port.
10. It is recommended to contact [My Oracle Support \(MOS\)](#) 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 \(MOS\)](#) 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)

**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 \(MOS\)](#) for assistance.

### 19803 - Communication Agent stack event queue utilization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <ComAgent StackTask Name>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | cAFQueueUtilNotify   |

#### Recovery:

1. Use **Main Menu > 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 \(MOS\)](#) for assistance.

2. Use **Main Menu > Status & Control > 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 \(MOS\)](#) 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 \(MOS\)](#) for assistance.

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

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | CAF  |
| <b>Description:</b> | 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.

- It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## 19805 - Communication Agent Failed To Align Connection

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | CAF   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | cAFConnAlignFailedNotify  |

### Recovery:

- If the connection administrative action is set to 'disable', the alarm is cleared. No further action is necessary.
- Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
- 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.
- Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
- 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.

- It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## 19806 - Communication Agent CommMessage mempool utilization

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | CAF   |
| <b>Description:</b> | The percent utilization of the Communication Agent CommMessage mempool is approaching defined threshold capacity.<br>The percent utilization of the Communication Agent internal resource pool (CommMessage) is approaching its defined capacity. If this problem persists and the usage reaches 100% utilization, ComAgent will allocate |

the CommMessage objects from the heap. This should not impact the functionality, but may impact performance and/or latency.

|                            |                         |
|----------------------------|-------------------------|
| <b>Severity:</b>           | Critical, Major, Minor  |
| <b>Instance:</b>           | <ComAgent Process Name> |
| <b>HA Score:</b>           | Normal                  |
| <b>Auto Clear Seconds:</b> | 0 (zero)                |
| <b>OID:</b>                | cAFPoolResUtilNotify    |

**Recovery:**

1. Use **Main Menu > 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 \(MOS\)](#) for assistance.

2. Use **Main Menu > Status & Control > 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 \(MOS\)](#) 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 \(MOS\)](#) for assistance.

**19807 - Communication Agent User Data FIFO Queue utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <ComAgent StackTask Name>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | cAFUserDataFIFOUtilNotify  |

**Recovery:**

1. 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.

2. Use **Main Menu > Alarms & Events** to determine if the ComAgent worker thread may be experiencing a problem preventing it from processing events from User Data FIFO queue.

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

3. The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from **Main Menu > Status & Control > KPIs**.

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

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

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 **Main Menu > Status & Control > KPIs**.

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 \(MOS\)](#) for assistance.

## 19808 - Communication Agent Connection FIFO Queue utilization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <ComAgent StackTask Name>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | cAFMxFIFOUtilNotify  |

### Recovery:

1. 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.
2. 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 Support \(MOS\)](#) for assistance.

3. The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from **Main Menu > Status & Control > KPIs**.

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

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

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 **Main Menu > Status & Control > KPIs**.

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 \(MOS\)](#) for assistance.

## 19810 - Communication Agent Egress Message Discarded

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | CAF  |
| <b>Description:</b>      | The Communication Agent egress message is being discarded due to one of the following reasons: <ul style="list-style-type: none"> <li>• Unknown destination server</li> <li>• Connection state is not InService</li> <li>• Incompatible destination</li> <li>• Serialization failed</li> <li>• MxEndpoint send failed</li> <li>• Internal error</li> </ul> |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <RemoteIP> <p><b>Note:</b> If &lt;RemoteIP&gt; is not known at the time of message discard, then "Unknown" will be used.</p>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance.

## 19811 - Communication Agent Ingress Message Discarded

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | Communication Agent Ingress Message Discarded. |

|                          |                                       |
|--------------------------|---------------------------------------|
| <b>Severity:</b>         | Info                                  |
| <b>Instance:</b>         | <RemoteIP>                            |
| <b>HA Score:</b>         | Normal                                |
| <b>Throttle Seconds:</b> | 10                                    |
| <b>OID:</b>              | cAFEventIngressMessageDiscardedNotify |

**Recovery:**

1. View the Event AddInfo 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 \(MOS\)](#) for assistance.

**19814 - Communication Agent Peer has not responded to heartbeat**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | Communication Agent Peer has not responded to heartbeat. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <RemoteIP>   |
| <b>HA Score:</b>    | Normal   |
| <b>OID:</b>         | 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 \(MOS\)](#) for assistance.

**19816 - Communication Agent Connection State Changed**

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | Communication Agent Connection State Changed. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <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 \(MOS\)](#) 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 \(MOS\)](#) 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:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 19820 - Communication Agent Routed Service Unavailable

**Alarm Group:** CAF

**Description:** This alarm indicates that 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. 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 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 \(MOS\)](#) 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 \(MOS\)](#) for assistance.

## 19822 - Communication Agent Routed Service Congested

**Alarm Group:** CAF

**Description:** This alarm indicates that 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. 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 are congested and the degree to which they are congested.
3. Check the far-end of the congested connections in order to further isolate the cause of congestion.

If the far-end servers are overloaded, then it is possible that 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 \(MOS\)](#) for assistance.

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

**Alarm Group:** CAF

|                            |   |
|----------------------------|---|
| <b>Description:</b>        | Communication Agent routed service is routing traffic using a connection group that has a lower-priority than another connection group. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <ServiceName>   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

**19824 - Communication Agent Pending Transaction Utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | The ComAgent Reliable Transfer Function is approaching or exceeding its engineered reliable transaction handling capacity. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | n/a (ComAgent process)   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | cAFTransUtilNotify   |

**Recovery:**

1. Use **Main Menu > Status & Control > 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 **Main Menu > Alarm & Events** and 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 \(MOS\)](#) for assistance.

## 19825 - Communication Agent Transaction Failure Rate

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | The number of failed transactions during the sampling period has exceeded configured thresholds. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <ServiceName>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | cAFTransFailRateNotify   |

### Recovery:

1. Use **Main Menu > Status & Control > 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 **Main Menu > Alarm & Events** and 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 \(MOS\)](#) for assistance.

## 19826 - Communication Agent Connection Congested

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | CAF   |
| <b>Description:</b>        | This alarm indicates that 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | cAFConnCongestedNotify  |

### 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.
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. If the Remote MP Overload Level (OL) > 0 then determine why the remote server is congested.
  - a) Verify that the remote server is not under maintenance.
  - b) Examine the remote's CPU utilization.
  - c) Examine the remote's current alarms.
5. If the local server's Transport Congestion Level (TCL) > 0 then determine why the connection is not handling the load.
  - a) The remote may be overload by traffic from other MPs.
  - b) The local server may be trying to send too much traffic to the remote.
  - c) The IP connectivity may be impaired.
6. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 19827 - SMS stack event queue utilization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SMS  |
| <b>Description:</b>        | The percent utilization of the SMS Task stack queue is approaching defined threshold capacity. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <SMS Thread/Queue Index>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

### 19830 - Communication Agent Service Registration State Change

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | Communication Agent Service Registration State Change. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <ServiceName>  |
| <b>HA Score:</b>    | Normal   |

**OID:** cAFEEventComAgtSvcRegChangedNotify

**Recovery:**

This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.

### 19831 - Communication Agent Service Operational State Changed

**Event Type:** CAF  
**Description:** Communication Agent Service Operational State Changed.  
**Severity:** Info  
**Instance:** <ServiceName>  
**HA Score:** Normal  
**OID:** cAFEEventComAgtSvcOpStateChangedNotify

**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 \(MOS\)](#) 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:** cAFEEventComAgtTransFailedNotify

**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 \(MOS\)](#) for assistance.

### 19833 - Communication Agent Service Egress Message Discarded

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | CAF  |
| <b>Description:</b>      | Communication Agent Service Egress Message Discarded.  |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ServiceName> <ul style="list-style-type: none"> <li>• If serviceID is unknown, then &lt;ServiceName&gt; is null.</li> </ul> |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance.

### 19842 - Communication Agent Resource-Provider Registered

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | Communication Agent Resource-Provider Registered. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <ResourceName>                                    |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | cAFEventResourceProviderRegisteredNotify          |

#### Recovery:

No action required.

**19843 - Communication Agent Resource-Provider Resource State Changed**

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | Communication Agent Resource-Provider Resource State Changed. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <ProviderServerName>: <ResourceName>                          |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | cAFEventResourceStateChangeNotify                             |
| <b>Recovery:</b>    | No action required.   |

**19844 - Communication Agent Resource-Provider Stale Status Received**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | CAF  |
| <b>Description:</b>      | Communication Agent Resource-Provider Stale Status Received.   |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ProviderServerName>: <ResourceName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | cAFEventStaleHBPacketNotify  |
| <b>Recovery:</b>         | 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**

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | Communication Agent Resource-Provider Deregistered. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <ResourceName>                                      |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | cAFEventResourceProviderDeRegisteredNotify          |
| <b>Recovery:</b>    | No action required.                                 |

## 19846 - Communication Agent Resource Degraded

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <ResourceName>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

## 19847 - Communication Agent Resource Unavailable

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | CAF   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <ResourceName>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | cAFResourceUnavailNotify  |

### Recovery:

1. Use **Main Menu > Communication Agent > Maintenance > Connection Status** to verify that 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, use **Main Menu > 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 that maintenance actions have been taken that have removed from service the application that provides the concerned resource.

3. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 19848 - Communication Agent Resource Error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | Communication Agent Resource Error. Two sets of servers are using incompatible configurations for a ComAgent resource. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | <ResourceName>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 50   |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

### 19850 - Communication Agent Resource-User Registered

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | Communication Agent Resource-User Registered. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <ResourceName>                                |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | cAFEventResourceUserRegisteredNotify          |

#### Recovery:

No action required.

### 19851 - Communication Agent Resource-User Deregistered

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | Communication Agent Resource-User Deregistered. |

**Severity:** Info  
**Instance:** <ResourceName>  
**HA Score:** Normal  
**OID:** cAFEventResourceUserDeRegisteredNotify  
**Recovery:**  
 No action required.

### 19852 - Communication Agent Resource Routing State Changed

**Event Type:** CAF  
**Description:** Communication Agent Resource Routing State Changed.  
**Severity:** Info  
**Instance:** <ResourceName>  
**HA Score:** Normal  
**OID:** cAFEventResourceRoutingStateNotify  
**Recovery:**  
 No action required.

### 19853 - Communication Agent Resource Egress Message Discarded

**Event Type:** CAF  
**Description:** Communication Agent Resource Egress Message Discarded.  
**Severity:** Info  
**Instance:** <ResourceName>: <SubResourceID>  
**Note:** If the resource is unknown, then <ResourceName> is the ResourceID converted to text. The <SubResourceID> is an integer converted to text, regardless of whether it is known or unknown.  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** cAFEventHaEgressMessageDiscardedNotify

**Recovery:**

1. Message is being discarded due to one of the reasons specified in Event AddInfo.

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 \(MOS\)](#) for assistance.

**19854 - Communication Agent Resource-Provider Tracking Table Audit Results**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | None   |
| <b>HA Score:</b>    | Normal   |
| <b>OID:</b>         | cAFEventHaRPTTAuditResultNotify  |
| <b>Recovery:</b>    | No action required.  |

**19855 - Communication Agent Resource Has Multiple Actives**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | CAF   |
| <b>Description:</b>        | 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.               |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <ResourceName>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | cAFMultipleActivesNotify  |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. Use <b>Main Menu &gt; Communication Agent &gt; Maintenance &gt; HA Services Status</b> to determine which Resource Provider servers are announcing 'Active' status for the Resource.</li> <li>2. Investigate possible IP network isolation between these Resource Provider servers.</li> <li>3. It is recommended to contact <a href="#">My Oracle Support (MOS)</a> for assistance.</li> </ol> |

**19856 - Communication Agent Service Provider Registration State Changed**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | The Communication Agent Service Provider Registration State has changed. |

|                  |                                      |
|------------------|--------------------------------------|
| <b>Severity:</b> | Info                                 |
| <b>Instance:</b> | <ServiceName>                        |
| <b>HA Score:</b> | Normal                               |
| <b>OID:</b>      | 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 \(MOS\)](#) for further assistance.

**19857 - Communication Agent Service Provider Operational State Changed**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | The Communication Agent Service Provider Operational State has Changed |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <ServiceName>  |
| <b>HA Score:</b>    | Normal   |
| <b>OID:</b>         | 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 \(MOS\)](#).

**19858 - Communication Agent Connection Rejected**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | CAF   |
| <b>Description:</b>      | The Communication Agent receives a connection request from an unknown server. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <RemoteIP>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 1800 (30 minutes)   |
| <b>OID:</b>              | cAFEventSvcProvOpStateChangedNotify   |

**Recovery:**

1. Verify network routes are correctly configured for ComAgent.
2. If assistance is required, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 19860 - Communication Agent Configuration Daemon Table Monitoring Failure

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | None   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | cAFTableMonitorFailureNotify   |

### 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. If conditions do not permit a forced failover of the active NOAM, it is recommended to contact [My Oracle Support \(MOS\)](#) 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 that the alarm has cleared.
6. If the alarm has not cleared, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## 19861 - Communication Agent Configuration Daemon Script Failure

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | CAF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | None   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |

**OID:** cAFScriptFailureNotify

**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 server.
3. If conditions do not permit a forced failover of the active NOAM, it is recommended to contact [My Oracle Support \(MOS\)](#) 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 that the alarm has cleared.
6. If the alarm has not cleared, it is recommended to contact [My Oracle Support \(MOS\)](#) 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 \(MOS\)](#) for further assistance.

## 19863 - Communication Agent Max Connections Limit In Connection Group Reached

**Event Group:** CAF

|                          |  |
|--------------------------|--|
| <b>Description:</b>      | The maximum number of connections per connection group limit has been reached. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <Connection group name>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 \(MOS\)](#) for further assistance.

**19864 - ComAgent Successfully Set Host Server Hardware Profile**

|                     |   |
|---------------------|---|
| <b>Event Group:</b> | CAF   |
| <b>Description:</b> | ComAgent successfully set the host server hardware profile. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | None  |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | 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 \(MOS\)](#).

**19865 - ComAgent Failed to Set Host Server Hardware Profile**

|                     |  |
|---------------------|--|
| <b>Event Group:</b> | CAF  |
| <b>Description:</b> | ComAgent failed to set the host server hardware profile. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | None   |
| <b>HA Score:</b>    | Normal   |
| <b>OID:</b>         | 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 \(MOS\)](#).

### 19866 - Communication Agent Peer Group Status Changed

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | CAF   |
| <b>Description:</b> | The Communication Agent Peer Group operational status has changed |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <PeerGroupName>   |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | cAFEventPeerGroupStatusChangeNotify                               |
| <b>Recovery:</b>    | This alarm is informational and no action is required.            |

### 19867 - Communication Agent Peer Group Egress Message Discarded

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | CAF   |
| <b>Description:</b>      | The Communication Agent Peer Group egress message is being discarded due to one of the following reasons: <ul style="list-style-type: none"> <li>• Unknown Peer Group</li> <li>• Peer Group Unavailable</li> <li>• Peer Congested</li> <li>• Reliability not supported</li> </ul> |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <PeerGroupName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | cAFEventPSEgressMessageDiscardedNotify  |
| <b>Recovery:</b>         | This alarm is informational and no action is required.  |

### 19868 - Communication Agent Connection Rejected - Incompatible Network

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | CAF  |
| <b>Description:</b> | 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:** cAFEEventConnectionRejectNotify

**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 \(MOS\)](#) 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. Use **Main Menu > Status & Control > 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. Use **Main Menu > Alarms & Events** to examine the alarm log.  
It is recommended to contact [My Oracle Support \(MOS\)](#) 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.

|                            |                               |
|----------------------------|-------------------------------|
| <b>Severity:</b>           | Major                         |
| <b>Instance:</b>           | N/A                           |
| <b>HA Score:</b>           | Normal                        |
| <b>Auto Clear Seconds:</b> | 0 (zero)                      |
| <b>OID:</b>                | dbcCfgDbValidationErrorNotify |

**Recovery:**

An unexpected condition has occurred while performing a database update, but database updates are still enabled.

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**19902 - CFG-DB Update Failure**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | STK  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | dbcCfgDbUpdateFailureNotify  |

**Recovery:**

An unexpected condition has occurred while performing a database update and database updates are disabled.

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**19903 - CFG-DB post-update Error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | STK   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |

**OID:** dbcCfgDbPostUpdateErrorNotify

**Recovery:**

An unexpected condition has occurred while performing a database update, but database updates are still enabled.

It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

An unexpected condition has occurred while performing a database update and database updates are disabled.

It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

Measurement subsystem initialization has failed for the specified measurement.

It is recommended to contact [My Oracle Support \(MOS\)](#) 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

|                            |   |
|----------------------------|---|
| <b>Event Type:</b>         | DIAG  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <Connection name>   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 120   |
| <b>OID:</b>                | 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

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAG  |
| <b>Description:</b>      | Test message is given to a non-test connection to be transmitted. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <Connection name>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 5   |
| <b>OID:</b>              | dbcDiagnosticMessageDiscardNotify                                 |

**Recovery:**

Update routing rules to exclude Test messages from being routed to non-test connection.

Test messages should be received and sent only on test connections.

## Diameter Alarms and Events (8000-8299, 22000-22350, 22900-22999, 25500-25899)

### 8000 - MpEvFsmException

#### 8000 - 001 - MpEvFsmException\_SocketFailure

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type:</b>      | DIAM                            |
| <b>Description:</b>     | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:001                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

#### 8000 - 002 - MpEvFsmException\_BindFailure

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:002                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

### 8000 - 003 - MpEvFsmException\_OptionFailure

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:003                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

### 8000 - 004 - MpEvFsmException\_AcceptorCongested

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:004                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

#### Recovery

This event is potentially caused by a network or upgrade event that resulted in a synchronization of peer connection attempts.

**Note:** The rate will ease over time as an increasing number of connections are accepted.

### 8000 - 101 - MpEvFsmException\_ListenFailure

|                    |                                 |
|--------------------|---------------------------------|
| <b>Event Type</b>  | DIAM                            |
| <b>Description</b> | DA-MP connection FSM exception. |
| <b>Severity</b>    | Info                            |
| <b>Instance</b>    | <DA-MP Name>:101                |

|                         |                                 |
|-------------------------|---------------------------------|
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**8000 - 102 - MpEvFsmException\_PeerDisconnected**

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:102                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery**

No action required.

**8000 - 103 - MpEvFsmException\_PeerUnreachable**

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:103                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery**

Potential causes for this event are:

- A host IP interface is down.
- A host IP interface is unreachable from the peer.
- A peer IP interface is down.
- A peer IP interface is unreachable from the host.

**8000 - 104 - MpEvFsmException\_CexFailure**

|                    |                                 |
|--------------------|---------------------------------|
| <b>Event Type</b>  | DIAM                            |
| <b>Description</b> | DA-MP connection FSM exception. |

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:104                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery**

Potential causes for this event are:

- The peer is misconfigured.
- The host is misconfigured.

**8000 - 105 - MpEvFsmException\_CerTimeout**

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:105                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery**

No action required.

**8000 - 106 - MpEvFsmException\_AuthenticationFailure**

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:106                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery**

Potential causes for this event are:

- The peer is misconfigured.
- The host is misconfigured.

**8000 - 201 - MpEvFsmException\_UdpSocketLimit**

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | DA-MP connection FSM exception. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <DA-MP Name>:201                |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvFsmException |

**Recovery:**

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**

|                         |                              |
|-------------------------|------------------------------|
| <b>Event Type</b>       | DIAM                         |
| <b>Description</b>      | DA-MP exception.             |
| <b>Severity</b>         | Info                         |
| <b>Instance</b>         | <DA-MP Name>:001             |
| <b>HA Score</b>         | Normal                       |
| <b>Throttle Seconds</b> | None                         |
| <b>OID</b>              | eagleXgDiameterMpEvException |

**Recovery**

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

**8002 - MpEvRxException****8002 - 001 - MpEvRxException\_DiamMsgPoolCongested**

|                    |   |
|--------------------|---|
| <b>Event Type</b>  | DIAM  |
| <b>Description</b> | DA-MP ingress message processing exception. |

|                         |                                |
|-------------------------|--------------------------------|
| <b>Severity</b>         | Info                           |
| <b>Instance</b>         | <DA-MP Name>:001               |
| <b>HA Score</b>         | Normal                         |
| <b>Throttle Seconds</b> | 10                             |
| <b>OID</b>              | eagleXgDiameterMpEvRxException |

**Recovery**

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**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:002                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

**Recovery**

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

**8002 - 003 - MpEvRxException\_CpuCongested**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:003                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

**Recovery**

Potential causes for this event are:

- One or more peers are generating more traffic than is nominally expected.
- Configuration requires more CPU for message processing than is nominally expected.

- One or more peers are answering slowly, causing a backlog of pending transactions

### 8002 - 004 - MpEvRxException\_SigEvPoolCongested

|                  |   |
|------------------|---|
| Event Type       | DIAM  |
| Description      | DA-MP ingress message processing exception. |
| Severity         | Info  |
| Instance         | <DA-MP Name>:004                            |
| HA Score         | Normal                                      |
| Throttle Seconds | 10  |
| OID              | eagleXgDiameterMpEvRxException              |

#### Recovery

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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

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

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:007                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

#### Recovery

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 8002 - 008 - MpEvRxException\_DrlAnsQueueCongested

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:008                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

#### Recovery

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 8002 - 009 - MpEvRxException\_ComAgentCongested

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:009                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

#### Recovery

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 8002 - 201 - MpEvRxException\_MsgMalformed

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:201                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

#### Recovery

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect.

### 8002 - 202 - MpEvRxException\_PeerUnknown

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:202                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterMpEvRxException              |

#### Recovery

The host or peer may be misconfigured. Adjust the peer IP address(es) option of the associated Peer Node if necessary.

### 8002 - 203 - MpEvRxException\_RadiusMsgPoolCongested

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:203                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

### 8002 - 204 - MpEvRxException\_ItrPoolCongested

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:204                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | 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 \(MOS\)](#).

**8002 - 205 - MpEvRxException\_RclRxTaskQueueCongested**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:205                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | 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 \(MOS\)](#).

**8002 - 206 - MpEvRxException\_RclSigEvPoolCongested**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | DA-MP ingress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <DA-MP Name>:206                            |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | 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 \(MOS\)](#).

**8002 - 207 - MpEvRxException\_ReqDuplicate**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:207                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | 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 \(MOS\)](#).

**8002 - 208 - MpEvRxException\_SharedSecretUnavailable**

|                         |                                 |
|-------------------------|---------------------------------|
| <b>Event Type</b>       | DIAM                            |
| <b>Description</b>      | Failed to access shared secret. |
| <b>Severity</b>         | Info                            |
| <b>Instance</b>         | <Connection Name>:208           |
| <b>HA Score</b>         | Normal                          |
| <b>Throttle Seconds</b> | 10                              |
| <b>OID</b>              | eagleXgDiameterMpEvRxException  |

**Recovery:**

Check to see if alarm 8207 is present. If so, follow the recovery steps for alarm [8207 - MpRadiusKeyError](#).

**8003 - MpEvTxException****8003 - 001 - MpEvTxException\_ConnUnknown**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                       |
| <b>Description</b>      | DA-MP egress message processing exception. |
| <b>Severity</b>         | Info                                       |
| <b>Instance</b>         | <DA-MP Name>:001                           |
| <b>HA Score</b>         | Normal                                     |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterMpEvTxException             |

**Recovery**

No action required.

**8003 - 101 - MpEvTxException\_DclTxTaskQueueCongested**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                       |
| <b>Description</b>      | DA-MP egress message processing exception. |
| <b>Severity</b>         | Info                                       |
| <b>Instance</b>         | <DA-MP Name>:101                           |
| <b>HA Score</b>         | Normal                                     |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterMpEvTxException             |

**Recovery**

This event is potentially caused by one or more peers being routed more traffic than is nominally expected.

**8003 - 201 - MpEvTxException\_RclTxTaskQueueCongested**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                       |
| <b>Description</b>      | DA-MP egress message processing exception. |
| <b>Severity</b>         | Info                                       |
| <b>Instance</b>         | <DA-MP Name>:201                           |
| <b>HA Score</b>         | Normal                                     |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | 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 \(MOS\)](#).

### 8003 - 202 - MpEvTxException\_EtrPoolCongested

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                       |
| <b>Description</b>      | DA-MP egress message processing exception. |
| <b>Severity</b>         | Info                                       |
| <b>Instance</b>         | <DA-MP Name>:202                           |
| <b>HA Score</b>         | Normal                                     |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | 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 \(MOS\)](#).

### 8003 - 203 - MpEvTxException\_RadiusMsgPoolCongested

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                       |
| <b>Description</b>      | DA-MP egress message processing exception. |
| <b>Severity</b>         | Info                                       |
| <b>Instance</b>         | <DA-MP Name>:203                           |
| <b>HA Score</b>         | Normal                                     |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

**8003 - 204 - MpEvTxException\_RadiusIdPoolCongested**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                       |
| <b>Description</b>      | DA-MP egress message processing exception. |
| <b>Severity</b>         | Info                                       |
| <b>Instance</b>         | <DA-MP Name>:204                           |
| <b>HA Score</b>         | Normal                                     |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | 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**

|                    |                                 |
|--------------------|---------------------------------|
| <b>Event Type</b>  | DIAM                            |
| <b>Description</b> | Failed to access shared secret. |
| <b>Severity</b>    | Info                            |
| <b>Instance</b>    | <DA-MP Name>:205                |

|                         |                                |
|-------------------------|--------------------------------|
| <b>HA Score</b>         | Normal                         |
| <b>Throttle Seconds</b> | 10                             |
| <b>OID</b>              | eagleXgDiameterMpEvTxException |

**Recovery:**

1. Proceed to [Step 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 \(MOS\)](#).

**8004 - EvFsmAdState****8004 - 001 - EvFsmAdState\_StateChange**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection FSM administrative state change. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:001                       |
| <b>HA Score</b>         | Normal                                      |
| <b>Throttle Seconds</b> | None  |
| <b>OID</b>              | eagleXgDiameterEvFsmAdState                 |

**Recovery**

No action required.

**8005 - EvFsmOpState****8005 - 001 - EvFsmOpState\_StateChange**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM                                     |
| <b>Description</b>      | Connection FSM operational state change. |
| <b>Severity</b>         | Info                                     |
| <b>Instance</b>         | <Connection Name>:001                    |
| <b>HA Score</b>         | Normal                                   |
| <b>Throttle Seconds</b> | None                                     |
| <b>OID</b>              | 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

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:001         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

#### Recovery

Potential causes of this event are:

- DNS server configuration is invalid.
- DNS server(s) are unavailable.
- DNS server(s) are unreachable.
- FQDN configuration is invalid.

### 8006 - 002 - EvFsmException\_ConnReleased

|                    |                           |
|--------------------|---------------------------|
| <b>Event Type</b>  | DIAM                      |
| <b>Description</b> | Connection FSM exception. |
| <b>Severity</b>    | Info                      |
| <b>Instance</b>    | <Connection Name>:002     |
| <b>HA Score</b>    | Normal                    |

|                         |                               |
|-------------------------|-------------------------------|
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

No action required.

**8006 - 101 - EvFsmException\_SocketFailure**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:101         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

**8006 - 102 - EvFsmException\_BindFailure**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:102         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

**8006 - 103 - EvFsmException\_OptionFailure**

|                    |                           |
|--------------------|---------------------------|
| <b>Event Type</b>  | DIAM                      |
| <b>Description</b> | Connection FSM exception. |

|                         |                               |
|-------------------------|-------------------------------|
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:103         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance.

**8006 - 104 - EvFsmException\_ConnectFailure**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:104         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**8006 - 105 - EvFsmException\_PeerDisconnected**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:105         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

No action required. Potential causes for this event are:

- Diameter peer signaled DPR.
- Peer is unavailable.

**8006 - 106 - EvFsmException\_PeerUnreachable**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:106         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

Potential causes for this event are:

- A host IP interface is down.
- A host IP interface is unreachable from the peer.
- A peer IP interface is down.
- A peer IP interface is unreachable from the host.

**8006 - 107 - EvFsmException\_CexFailure**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:107         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

Potential causes for this event are:

- The peer is misconfigured.
- The host is misconfigured.

**8006 - 108 - EvFsmException\_CeaTimeout**

|                    |                           |
|--------------------|---------------------------|
| <b>Event Type</b>  | DIAM                      |
| <b>Description</b> | Connection FSM exception. |
| <b>Severity</b>    | Info                      |
| <b>Instance</b>    | <Connection Name>:108     |
| <b>HA Score</b>    | Normal                    |

**Throttle Seconds** 10  
**OID** eagleXgDiameterEvFsmException

**Recovery**

No action required.

**8006 - 109 - EvFsmException\_DwaTimeout**

**Event Type** DIAM  
**Description** Connection FSM exception.  
**Severity** Info  
**Instance** <Connection Name>:109  
**HA Score** Normal  
**Throttle Seconds** 10  
**OID** eagleXgDiameterEvFsmException

**Recovery**

No action required.

**8006 - 110 - EvFsmException\_DwaTimeout**

**Event Type** DIAM  
**Description** Connection FSM exception.  
**Severity** Info  
**Instance** <Connection Name>:110  
**HA Score** Normal  
**Throttle Seconds** 10  
**OID** eagleXgDiameterEvFsmException

**Recovery**

No action required.

**8006 - 111 - EvFsmException\_ProvingFailure**

**Event Type** DIAM  
**Description** Connection FSM exception.  
**Severity** Info  
**Instance** <Connection Name>:111  
**HA Score** Normal  
**Throttle Seconds** 10  
**OID** eagleXgDiameterEvFsmException

**Recovery**

Potential causes for this event are:

- A host IP interface is unreachable from the peer, or intermittently so.
- A peer IP interface is unreachable from the host, or intermittently so.

**8006 - 112 - EvFsmException\_WatchdogFailure**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:112         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

Potential causes for this event are:

- A host IP interface is unreachable from the peer, or intermittently so.
- A peer IP interface is unreachable from the host, or intermittently so.

**8006 - 113 - EvFsmException\_AuthenticationFailure**

|                         |                               |
|-------------------------|-------------------------------|
| <b>Event Type</b>       | DIAM                          |
| <b>Description</b>      | Connection FSM exception.     |
| <b>Severity</b>         | Info                          |
| <b>Instance</b>         | <Connection Name>:113         |
| <b>HA Score</b>         | Normal                        |
| <b>Throttle Seconds</b> | 10                            |
| <b>OID</b>              | eagleXgDiameterEvFsmException |

**Recovery**

Potential causes for this event are:

- The peer is misconfigured.
- The host is misconfigured.

**8007 - EvException****8007 - 101 - EvException\_MsgPriorityFailure**

|                         |                            |
|-------------------------|----------------------------|
| <b>Event Type</b>       | DIAM                       |
| <b>Description</b>      | Connection exception.      |
| <b>Severity</b>         | Info                       |
| <b>Instance</b>         | <Connection Name>:101      |
| <b>HA Score</b>         | Normal                     |
| <b>Throttle Seconds</b> | 10                         |
| <b>OID</b>              | eagleXgDiameterEvException |

**Recovery**

This event is potentially caused by misconfiguration of the host.

**8008 - EvRxException****8008 - 001 - EvRxException\_MaxMpsExceeded**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:001                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery**

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

**8008 - 101 - EvRxException\_MsgMalformed**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:101                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**8008 - 102 - EvRxException\_MsgInvalid**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:102                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**8008 - 201 - EvRxException\_SharedSecretUnavailable**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:201                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.  
The peer may have an implementation defect.

**8008 - 202 - EvRxException\_MsgAttrLenUnsupported**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:202                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect.

### 8008 - 203 - EvRxException\_MsgTypeUnsupported

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:203                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

#### Recovery:

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect or may be misconfigured.

### 8008 - 204 - EvRxException\_AnsOrphaned

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:204                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

#### Recovery:

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

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:205                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect.

**8008 - 206 - EvRxException\_StatusAuthMissing**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:206                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect.

**8008 - 207 - EvRxException\_MsgAuthInvalid**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:207                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | 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 \(MOS\)](#) for assistance. This event is unexpected.

**8008 - 208 - EvRxException\_ReqAuthInvalid**

|                    |  |
|--------------------|--|
| <b>Event Type</b>  | DIAM   |
| <b>Description</b> | Connection ingress message processing exception. |
| <b>Severity</b>    | Info   |

|                         |                              |
|-------------------------|------------------------------|
| <b>Instance</b>         | <Connection Name>:208        |
| <b>HA Score</b>         | Normal                       |
| <b>Throttle Seconds</b> | 10                           |
| <b>OID</b>              | eagleXgDiameterEvRxException |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may be misconfigured.

**8008 - 209 - EvRxException\_AnsAuthInvalid**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:209                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may be misconfigured.

**8008 - 210 - EvRxException\_MsgAttrAstUnsupported**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:210                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

**Recovery:**

1. This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:212                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

#### Recovery:

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer or host is misconfigured.

### 8008 - 213 - EvRxException\_ConnUnavailable

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DIAM   |
| <b>Description</b>      | Connection ingress message processing exception. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | <Connection Name>:213                            |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 10   |
| <b>OID</b>              | eagleXgDiameterEvRxException                     |

#### Recovery:

No action required. This event is for informational purposes only.

## 8009 - EvTxException

### 8009 - 001 - EvTxException\_ConnUnavailable

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:001                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |

**OID** eagleXgDiameterEvTxException

**Recovery**

No action required.

**8009 - 101 - EvTxException\_DclTxConnQueueCongested**

**Event Type** DIAM  
**Description** Connection egress message processing exception.  
**Severity** Info  
**Instance** <Connection Name>:101  
**HA Score** Normal  
**Throttle Seconds** 10  
**OID** eagleXgDiameterEvTxException

**Recovery**

This event is potentially caused by a peer being routed more traffic than is nominally expected.

**8009 - 102 - EvTxException\_DtlsMsgOversized**

**Event Type** DIAM  
**Description** Connection egress message processing exception.  
**Severity** Info  
**Instance** <Connection Name>:102  
**HA Score** Normal  
**Throttle Seconds** 10  
**OID** eagleXgDiameterEvTxException

**Recovery**

This event is potentially caused by a peer being routed more traffic than is nominally expected.

**8009 - 201 - EvTxException\_MsgAttrLenUnsupported**

**Event Type** DIAM  
**Description** Connection egress message processing exception.  
**Severity** Info  
**Instance** <Connection Name>:201  
**HA Score** Normal  
**Throttle Seconds** 10  
**OID** eagleXgDiameterEvTxException

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect.

**8009 - 202 - EvTxException\_MsgTypeUnsupported**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:202                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterEvTxException                    |

**Recovery:**

This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance. The peer may have an implementation defect, or may be misconfigured.

**8009 - 203 - EvTxException\_MsgLenInvalid**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:203                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterEvTxException                    |

**Recovery:**

1. This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

|                    |   |
|--------------------|---|
| <b>Event Type</b>  | DIAM  |
| <b>Description</b> | Connection egress message processing exception. |
| <b>Severity</b>    | Info  |

|                         |                              |
|-------------------------|------------------------------|
| <b>Instance</b>         | <Connection Name>:204        |
| <b>HA Score</b>         | Normal                       |
| <b>Throttle Seconds</b> | 10                           |
| <b>OID</b>              | eagleXgDiameterEvTxException |

**Recovery:**

1. This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:205                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterEvTxException                    |

**Recovery:**

1. This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:206                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterEvTxException                    |

**Recovery:**

1. This event is unexpected. It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:207                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterEvTxException                    |

**Recovery:**

No action required.

**8009 - 208 - EvTxException\_WriteFailure**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DIAM  |
| <b>Description</b>      | Connection egress message processing exception. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | <Connection Name>:208                           |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 10  |
| <b>OID</b>              | eagleXgDiameterEvTxException                    |

**Recovery:**

1. This event is unexpected. It is recommend to contact [My Oracle Support \(MOS\)](#) 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**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | DA-MP ingress message discarded or rejected. |
| <b>Severity</b>           | Major  |
| <b>Instance</b>           | <DA-MP Name>                                 |
| <b>HA Score</b>           | Normal                                       |
| <b>Auto Clear Seconds</b> | 30   |
| <b>OID</b>                | eagleXgDiameterMpIngressDrop                 |

**Recovery**

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

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | Connection egress message rate threshold crossed. |
| <b>Severity</b>           | Minor, Major, Critical                            |
| <b>Instance</b>           | <Connection Name>                                 |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | eagleXgDiameterEmr                                |

#### Recovery

This alarm is potentially caused when a peer is routed more traffic than is nominally expected.

### 8012 - MpRxNgnPsOfferedRate

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | DA-MP ingress NGN-PS message rate threshold crossed. |
| <b>Severity</b>           | Major  |
| <b>Instance</b>           | MpRxNgnPsOfferedRate, DIAM                           |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | eagleXgDiameterMpRxNgnPsOfferedRateNotify            |

#### Recovery

Potential causes of this alarm:

- 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.

The alarm will clear when threshold crossing abates.

### 8013 - MpNgnPsStateMismatch

|                    |      |
|--------------------|------|
| <b>Alarm Group</b> | DIAM |
|--------------------|------|

|                           |   |
|---------------------------|---|
| <b>Description</b>        | DA-MP NGN-PS administrative and operational state mismatch. |
| <b>Severity</b>           | Major   |
| <b>Instance</b>           | <DA-MP Name>  |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | eagleXgDiameterMpNgnPsStateMismatchNotify                   |

**Recovery**

This alarm is potentially caused when a DA-MP restart is required.

The alarm will clear when administrative and operational states are aligned.

**8014 - MpNgnPsDrop**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | DA-MP NGN-PS message discarded or rejected. |
| <b>Severity</b>           | Major                                       |
| <b>Instance</b>           | <DA-MP Name>                                |
| <b>HA Score</b>           | Normal                                      |
| <b>Auto Clear Seconds</b> | 30  |
| <b>OID</b>                | eagleXgDiameterMpNgnPsDropNotify            |

**Recovery**

Potential causes of this alarm are:

- Routing or application controls are configured incorrectly.
- Peer or network is in congestion.
- Engineering of internal resources is insufficient.

**8015 - NgnPsMsgMisrouted**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | NGN-PS message routed to peer DSR lacking NGN-PS support. |
| <b>Severity</b>           | Major   |
| <b>Instance</b>           | <Connection Name>   |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 30  |
| <b>OID</b>                | eagleXgDiameterNgnPsMsgMisroutedNotify                    |

**Recovery**

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.

**8100 - NormMsgMisrouted**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAG  |
| <b>Description:</b>        | Normal message routed onto diagnostic connection. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <Connection Name>                                 |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 30 (after last occurrence)                        |
| <b>OID:</b>                | 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 \(MOS\)](#).

**8101 - DiagMsgMisrouted**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAG  |
| <b>Description:</b>        | Diagnostic message routed onto normal connection. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <Connection Name>                                 |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 30 (after last occurrence)                        |
| <b>OID:</b>                | 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 \(MOS\)](#).

**8200 - MpRadiusMsgPoolCongested**

|                    |  |
|--------------------|--|
| <b>Alarm Group</b> | DIAM   |
| <b>Description</b> | DA-MP RADIUS message pool utilization threshold crossed. |
| <b>Severity</b>    | Minor, Major, Critical                                   |

|                           |   |
|---------------------------|---|
| <b>Instance</b>           | MpRadiusMsgPool, DIAM                   |
| <b>HA Score</b>           | Normal                                  |
| <b>Auto Clear Seconds</b> | 0 (zero)                                |
| <b>OID</b>                | 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 \(MOS\)](#).

**8201 - RclRxTaskQueueCongested**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | RCL ingress task message queue utilization threshold crossed. |
| <b>Severity</b>           | Minor, Major, Critical  |
| <b>Instance</b>           | RclRxTaskQueue, DIAM  |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | 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 \(MOS\)](#).

**8202 - RclItrPoolCongested**

|                    |   |
|--------------------|---|
| <b>Alarm Group</b> | DIAM  |
| <b>Description</b> | RCL ITR pool utilization threshold crossed. |
| <b>Severity</b>    | Minor, Major, Critical                      |

|                           |                                    |
|---------------------------|------------------------------------|
| <b>Instance</b>           | RclItrPool, DIAM                   |
| <b>HA Score</b>           | Normal                             |
| <b>Auto Clear Seconds</b> | 0 (zero)                           |
| <b>OID</b>                | 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 \(MOS\)](#).

**8203 - RclRxTaskQueueCongested**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM                                   |
| <b>Description</b>        | RCL egress task threshold crossed.     |
| <b>Severity</b>           | Minor, Major, Critical                 |
| <b>Instance</b>           | RclRxTaskQueue, DIAM                   |
| <b>HA Score</b>           | Normal                                 |
| <b>Auto Clear Seconds</b> | 0 (zero)                               |
| <b>OID</b>                | eagleXgDiameterRclRxTaskQueueCongested |

**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 \(MOS\)](#).

**8204 - RclEtrPoolCongested**

|                    |   |
|--------------------|---|
| <b>Alarm Group</b> | DIAM  |
| <b>Description</b> | RCL ETR pool utilization threshold crossed. |

|                           |                                    |
|---------------------------|------------------------------------|
| <b>Severity</b>           | Minor, Major, Critical             |
| <b>Instance</b>           | RclEtrPool, DIAM                   |
| <b>HA Score</b>           | Normal                             |
| <b>Auto Clear Seconds</b> | 0 (zero)                           |
| <b>OID</b>                | 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 \(MOS\)](#).

**8205 - RadiusXactionFail**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | 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. |
| <b>Severity</b>           | Minor, Major  |
| <b>Instance</b>           | <Connection Name>   |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | 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**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | RADIUS average ingress message length threshold crossed. |
| <b>Severity</b>           | Minor, Major   |
| <b>Instance</b>           | MpRxRadiusAllLen, DIAM                                   |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | 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**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | DA-MP RADIUS key error. This alarm is unexpected during normal processing. The presence of this alarm indicates that the DSR encountered an error while accessing RADIUS encryption keys that are used to decrypt RADIUS shared secrets. |
| <b>Severity</b>           | Critical   |
| <b>Instance</b>           | <DA-MP Name>   |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | eagleXgDiameterMpRadiusKeyError  |

**Recovery:**

1. Synchronize the RADIUS key file.
2. Restart the DSR process. If the required keys are now available, the alarm will not be raised.
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22001 - Message Decoding Failure**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | DIAM   |
| <b>Description:</b> | A message received from a peer was rejected because of a decoding failure. Decoding failures can include missing mandatory parameters. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <TransConnName>  |

**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterIngressMsgRejectedDecodingFailureNotify

**Recovery:**

During Diameter Request decoding, the message content was inconsistent with the "Message Length" in the message header. This protocol violation can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

**22002 - Peer Routing Rules with Same Priority**

**Event Type:** DIAM  
**Description:** A peer routing table search with a received Request message found more than one highest priority Peer Routing Rule match. The system selected the first rule found but it is not guaranteed that the same rule will be selected in the future. It is recommended that Peer Routing Rules be unique for the same type of messages to avoid non-deterministic routing results.  
**Severity:** Info  
**Instance:** <MPName>  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterPeerRoutingTableRulesSamePriorityNotify

**Recovery:**

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:**

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 \(MOS\)](#) for assistance.

## 22005 - No peer routing rule found

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM  |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MPName>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterNoPrtRuleNotify  |

### Recovery:

1. Either the message was incorrectly routed to this node or additional Peer Routing Rules need to be added. Existing Peer Routing Rules can be viewed and updated using **Diameter > Configuration > Peer Routing Rules** page.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 22007 - Inconsistent Application ID Lists from a Peer

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <PeerName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterSupportedAppIdsInconsistentNotify   |

### Recovery:

1. A peer with multiple transport connections has established a connection and provided a list of supported Application IDs which does not 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 \(MOS\)](#).

### 22008 - Orphan Answer Response Received

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <TransConnName>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterOrphanAnswerResponseReceivedNotify  |
| <b>Recovery:</b>         | If this event is occurring frequently, the transaction timers may be set too low. The timer values can be viewed and/or modified using the <b>Diameter &gt; Configuration &gt; Pending Answer Timers</b> page.   |

### 22009 - Application Routing Rules with Same Priority

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 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 \(MOS\)](#).

## 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 \(MOS\)](#) for assistance.

## 22012 - Specified MCCA not provisioned

**Event Type:** DIAM

**Description:** The Message Copy Config Set specified by the trigger point is not provisioned.

**Severity:** Info

**Instance:** <MCCA>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterSpecifiedMCCANotProvisionedNotify

**Recovery:**

1. Verify the configured value of MCCA with the trigger point.
2. Verify the Message Copy CfgSet (MCCA) provisioning is properly configured.
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22013 - DAS Peer Number of Retransmits Exceeded for Copy**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM  |
| <b>Description:</b>      | The configured number of Message Copy retransmits has been exceeded for the DAS Peer.   |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MCCS>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>Note:</b>             | Because many route lists can be created on a DA-MP server, care must be taken to prevent excessive event generation with these resources. |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance.

**22014 - No DAS Route List specified**

|                          |   |
|--------------------------|---|
| <b>Alarm Group:</b>      | DIAM  |
| <b>Description:</b>      | No valid DAS Route List was specified in the Message Copy Config Set. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <RouteListId>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterNoDasRouteListSpecifiedNotify                          |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**22016 - Peer Node Alarm Aggregation Threshold**

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | DIAM |
|---------------------|------|

|                            |   |
|----------------------------|---|
| <b>Description:</b>        | This alarm occurs when there are a 'Critical' number of Peer Node alarms for a single Network Element.<br><br><b>Note:</b> The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the <b>Main Menu &gt; Diameter &gt; Configuration &gt; System Options</b> screen. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | <NetworkElement>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterPeerNodeUnavailableThresholdReachedNotify  |

**Recovery:**

1. Use **Main Menu > Diameter > Maintenance > Peer Nodes** to monitor Peer status.
2. Verify that 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 that the peer is not under maintenance.
5. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22017 - Route List Alarm Aggregation Threshold**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | This alarm occurs when there are a 'Critical' number of Route List alarms for the Network Element.<br><br><b>Note:</b> The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the <b>Main Menu &gt; Diameter &gt; Configuration &gt; System Options</b> screen. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | <NetworkElement>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

**22018 - Maintenance Leader HA Notification to go Active**

|                          |   |
|--------------------------|---|
| <b>Alarm Group:</b>      | DIAM  |
| <b>Description:</b>      | This alarm occurs when a DA-MP has received a notification from HA that the Maintenance Leader resource should transition to the Active role. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MP Node ID>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 1   |
| <b>OID:</b>              | eagleXgDiameterDaMpLeaderGoActiveNotificationNotify   |
| <b>Recovery:</b>         | No action necessary.  |

**22019 - Maintenance Leader HA Notification to go OOS**

|                          |  |
|--------------------------|--|
| <b>Alarm Group:</b>      | DIAM   |
| <b>Description:</b>      | This alarm occurs when a DA-MP has received a notification from HA that the Maintenance Leader resource should transition to the OOS role. |
| <b>Instance:</b>         | <MP Node ID>   |
| <b>Severity:</b>         | Info   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 1  |
| <b>OID:</b>              | eagleXgDiameterDaMpLeaderGoOOSNotificationNotify   |
| <b>Recovery:</b>         | No action necessary.   |

**22020 - Copy Message size exceeded the system configured size limit**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | DIAM   |
| <b>Description:</b> | The generated Copy message size exceeded the max message size on the system. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <DA-MP>  |
| <b>HA Score:</b>    | 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 \(MOS\)](#) 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 \(MOS\)](#).

## 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 which has already processed the message (it should examine the Route-Record AVPs prior to 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 \(MOS\)](#).

**22051 - Peer Unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | Unable to access the Diameter Peer because all of the transport connections are Down. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | <PeerName> (of the Peer which failed)   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterPeerUnavailableNotify  |

**Recovery:**

1. Peer status can be monitored from **Diameter > Maintenance > Peer Nodes**.
2. Verify that 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 that the peer is not under maintenance.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22052 - Peer Degraded**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <PeerName> (of the Peer which is degraded)  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterPeerDegradedNotify   |

**Recovery:**

1. Peer status can be monitored from **Diameter > Maintenance > Peer Nodes**.
2. Verify that 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 that the peer is not under maintenance.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22053 - Route List Unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | <p>The Route List is 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.</p> <p>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.</p> |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | <RouteListName> (of the Route List which failed)  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterRouteListUnavailableNotify   |

**Recovery:**

1. Route List status 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 peers in the Route List not under maintenance.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22054 - Route List Degraded**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | DIAM   |
| <b>Description:</b> | <p>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:</p> <ol style="list-style-type: none"> <li>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 will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for</li> </ol> |

Responder-Only mode, the peer will be 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. 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 peers in the Route List not under maintenance.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 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 \(MOS\)](#).

## 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, contact [My Oracle Support \(MOS\)](#).

## 22057 - ETG Rate Limit Degraded

**Alarm Group:** DIAM

**Description:** The ETG Rate Limit has exceeded the defined threshold.

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Major                                     |
| <b>Instance:</b>           | <ETGName>                                 |
| <b>HA Score:</b>           | Normal                                    |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                  |
| <b>OID:</b>                | eagleXgDiameterEtgRateLimitDegradedNotify |

**Recovery:**

1. Check the configuration in **Main Menu > Diameter > Configuration > Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Main Menu > Diameter > Maintenance > Egress Throttle Groups** and **Main Menu > Diameter > Maintenance > Connections** to determine if the sending Peers/Connections are offering too much traffic.
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22058 - ETG Pending Transaction Limit Degraded**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | The ETG Pending Transactions Limit has exceeded the defined threshold. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <ETGName>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterEtgPendingTransLimitDegradedNotify                      |

**Recovery:**

1. Check the configuration in **Main Menu > Diameter > Configuration > Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Main Menu > 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, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22059 - Egress Throttle Group Message Rate Congestion Level changed**

|                     |  |
|---------------------|--|
| <b>Event Group:</b> | DIAM   |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | 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 **Main Menu > Diameter > Configuration > Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Main Menu > Diameter > Maintenance > Egress Throttle Groups** and/or **Main Menu > 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 \(MOS\)](#) 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 **Main Menu > Diameter > Configuration > Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Main Menu > Diameter > Maintenance > Egress Throttle Groups** and/or **Main Menu > 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 \(MOS\)](#) for assistance.

**22061 - Egress Throttle Group Monitoring stopped**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | ETG Rate and Pending Transaction Monitoring is stopped on all configured ETGs |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <DA-MP Hostname>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterEtgMonitoringStoppedNotify                                     |

**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 **Main Menu > Communication Agent > Maintenance**.
2. Verify that ComAgent links are established between DA-MPs under **Main Menu > Communication Agent > Maintenance**
3. Verify the No-MP Leader condition in **Main Menu > 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 \(MOS\)](#).

**22062 - Actual Host Name cannot be determined for Topology Hiding**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | Diameter   |
| <b>Description:</b>      | Topology Hiding could not be applied because the Actual Host Name could not be determined. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <CfgSetName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 \(MOS\)](#).

**22063 - Diameter Max Message Size Limit Exceeded**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM  |
| <b>Description:</b>      | The size of the message encoded by DSR has exceeded its max limits. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <TransConnName>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterDiameterMaxMsgSizeLimitExceededNotify                |

**Recovery:**

No action required. However, if this event is seen to be incrementing consistently, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22064 - Upon receiving Redirect Host Notification the Request has not been submitted for re-routing**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <PeerName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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 \(MOS\)](#)

**22065 - Upon receiving Redirect Realm Notification the Request has not been submitted for re-routing**

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | DIAM  |
| <b>Description:</b> | The Redirect Realm Notification received is accepted but cannot be processed due to some reason, such as internal resources exhaustion. |
| <b>Severity:</b>    | Info  |

|                          |   |
|--------------------------|---|
| <b>Instance:</b>         | <PeerName>                                    |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | 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 \(MOS\)](#)

**22066 - ETG-ETL Scope Inconsistency**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | An ETG's Control Scope is set to ETL, but the ETG is not configured against an ETL. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <ETG Name>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22067 - ETL-ETG Invalid Association**

|                            |   |
|----------------------------|---|
| <b>Event Type:</b>         | DIAM  |
| <b>Description:</b>        | An ETL is associated with an ETG that does not exist. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <ETL Name>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22068 - TtpEvDoicException****22068 - 001 - TtpEvDoicException: DOIC OC-Supported-Features AVP not received**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM                                    |
| <b>Description:</b>      | DOIC Protocol Error                     |
| <b>Severity:</b>         | Info                                    |
| <b>Instance:</b>         | <TTP Name>:001                          |
| <b>HA Score:</b>         | Normal                                  |
| <b>Throttle Seconds:</b> | 10                                      |
| <b>OID:</b>              | eagleXgDiameterTtpEvDoicExceptionNotify |

**Recovery:**

The Peer Node associated with the TTP is not responding to a DOIC Capability Announcement (DCA). This can occur when the Peer Node either does not support DOIC or DOIC has been disabled on the Peer Node. The operator should either disable DOIC on the DSR associated with TTP by setting the TTP's "Dynamic Throttling Admin State" to Disabled or enable DOIC on the Peer Node.

**22068 - 002 - TtpEvDoicException: DOIC OC-Feature-Vector AVP contains an invalid value**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM                                    |
| <b>Description:</b>      | DOIC Protocol Error                     |
| <b>Severity:</b>         | Info                                    |
| <b>Instance:</b>         | <TTP Name>:002                          |
| <b>HA Score:</b>         | Normal                                  |
| <b>Throttle Seconds:</b> | 10                                      |
| <b>OID:</b>              | eagleXgDiameterTtpEvDoicExceptionNotify |

**Recovery:**

The Peer Node associated with the TTP has selected a DOIC Abatement Algorithm not supported by the TTP. This should never happen and may be the result of a mis-configuration or bug on the Peer Node. If this error persists, the operator should disable DOIC for the TTP by setting the TTP's "Dynamic Throttling Admin State" to Disabled or enable DOIC on the Peer Node.

**22068 - 003 - TtpEvDoicException: DOIC OC-Report-Type AVP contains an unsupported value**

|                     |                     |
|---------------------|---------------------|
| <b>Event Type:</b>  | DIAM                |
| <b>Description:</b> | DOIC Protocol Error |
| <b>Severity:</b>    | Info                |

**Instance:** <TTP Name>:003  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterTtpEvDoicExceptionNotify

**Recovery:**

The Peer Node associated with the TTP is sending a DOIC overload report which is not supported by DSR at this time. The operator should disable Realm-based DOIC overload reports on the Peer Node.

### 22068 - 004 - TtpEvDoicException: DOIC OC-Sequence-Number AVP contains an out of order sequence number

**Event Type:** DIAM  
**Description:** DOIC Protocol Error  
**Severity:** Info  
**Instance:** <TTP Name>:004  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterTtpEvDoicExceptionNotify

**Recovery:**

The Peer Node associated with the TTP has sent a DOIC overload report which 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:**

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**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM                                    |
| <b>Description:</b>      | DOIC Protocol Error                     |
| <b>Severity:</b>         | Info                                    |
| <b>Instance:</b>         | <TTP Name>:006                          |
| <b>HA Score:</b>         | Normal                                  |
| <b>Throttle Seconds:</b> | 10                                      |
| <b>OID:</b>              | eagleXgDiameterTtpEvDoicExceptionNotify |

**Recovery:**

The Peer Node associated with the TTP has sent a DOIC overload report containing an OC-Validity-Duration AVP value greater than the maximum allowed. The maximum value for the OC-Validity-Duration AVP is 86,400 seconds (24 hours). If this error occurs infrequently, then there may be a DOIC software error in the Peer Node. If this error occurs frequently, then the error may be caused by a Peer Node DOIC mis-configuration problem.

**22069 - TtpEvDoicOlr****22069 - 001 - TtpEvDoicOlr: Valid DOIC OLR Applied to TTP**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | A DOIC OverLoad Request (OLR) was received from a Peer Node and applied to a configured TTP. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <TTP Name>:001   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 0 (zero)   |
| <b>OID:</b>              | eagleXgDiameterTtpEvDoicExceptionNotify  |

**Recovery:**

No action required.

**22070 - TtpEvDegraded****22070 - 001 - TtpEvDegraded: TTP Degraded, Peer Overload**

|                     |              |
|---------------------|--------------|
| <b>Event Type:</b>  | DIAM         |
| <b>Description:</b> | TTP Degraded |

**Severity:** Info  
**Instance:** <TTP Name>:001  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** eagleXgDiameterTtpEvDegradedNotify  
**Recovery:**  
 No action required.

### 22070 - 002 - TtpEvDegraded: TTP Degraded, Peer Overload Recovery

**Event Type:** DIAM  
**Description:** TTP Degraded  
**Severity:** Info  
**Instance:** <TTP Name>:002  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** eagleXgDiameterTtpEvDegradedNotify  
**Recovery:**  
 No action required.

### 22070 - 003 - TtpEvDegraded: TTP Degraded, Static Rate Limit Exceeded

**Event Type:** DIAM  
**Description:** TTP Degraded  
**Severity:** Info  
**Instance:** <TTP Name>:003  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** eagleXgDiameterTtpEvDegradedNotify  
**Recovery:**  
 No action required.

### 22071 - TtgEvLossChg

#### 22071 - 001 - TtgEvLossChg: TTG Loss Percent Changed

**Event Type:** DIAM

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | TTG's Loss Percentage was modified.     |
| <b>Severity:</b>         | Info                                    |
| <b>Instance:</b>         | <TTG Name>:001                          |
| <b>HA Score:</b>         | Normal                                  |
| <b>Throttle Seconds:</b> | 0 (zero)                                |
| <b>OID:</b>              | eagleXgDiameterTtpEvDoicExceptionNotify |
| <b>Recovery:</b>         | No action required.                     |

### 22072 - TTP Degraded

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | The TTP's Operational Status has been changed to Degraded. |
| <b>Severity</b>           | Major  |
| <b>Instance</b>           | <TTP Name>   |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0  |
| <b>OID</b>                | eagleXgDiameterTtpDegradedNotify                           |
| <b>Recovery</b>           | No action required.  |

### 22073 - TTP Throttling Stopped

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | TTP rate throttling has been suspended due to an internal failure.   |
| <b>Severity</b>           | Minor  |
| <b>Instance</b>           | <DA-MP Name>   |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0  |
| <b>OID</b>                | eagleXgDiameterTtpThrottlingStoppedNotify  |
| <b>Recovery:</b>          | <ol style="list-style-type: none"> <li>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 <b>Main Menu &gt; Communication Agent &gt; Maintenance</b>.</li> <li>2. Verify that ComAgent links are established between DA-MPs under <b>Main Menu &gt; Communication Agent &gt; Maintenance</b></li> </ol> |

3. Verify the No-MP Leader condition in **Main Menu > 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 \(MOS\)](#).

### 22074 - TTP Maximum Loss Percentage Threshold Exceeded

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | The Maximum Loss Percentage Threshold assigned to the TTP has been exceeded. |
| <b>Severity</b>           | Major  |
| <b>Instance</b>           | <TTP Name>   |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0  |
| <b>OID</b>                | eagleXgDiameterTtpMaxLossPercentageExceededNotify                            |
| <b>Recovery</b>           | No action required.  |

### 22075 - Message is not routed to Application

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | ART Rule-X was selected but message was not routed because DSR Application is Disabled or not Available. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <DSR Application Name>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0  |
| <b>OID:</b>                | eagleXgDiameterArtMatchAppUnavailableNotify  |

#### Recovery:

1. Check the Application Status by selecting **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 \(MOS\)](#).

### 22077 - MpExcessiveRerouteRate

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | DIAM |
|---------------------|------|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | Request reroutes due to Answer response and/or Answer timeout having exceeded the configured onset threshold percentage on the DA-MP server. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | MpReroutePercent   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 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:** eagleXgDiameterMpReroutePercentNotify

**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 \(MOS\)](#).

## 22078 - Loop or Maximum Depth Exceeded in ART or PRT Search

|                          |   |
|--------------------------|---|
| <b>Alarm Group:</b>      | DIAM  |
| <b>Description:</b>      | An ART/PRT search has resulted in either a loop between ART/PRT tables, or the search depth has exceeded the maximum allowed depth. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MPName>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 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 \(MOS\)](#).

## 22101 - FsmOpStateUnavailable

**Alarm Group:** DIAM

**Description:** Connection is unavailable for Diameter Request/ Answer exchange with peer.

**Note:** This alarm is not added when the "Suppress Connection Unavailable Alarm" for a Transport Connection is set to "Yes".

**Severity:** Major

**Instance:** <Connection Name>

**HA Score:** Normal

**Auto Clear Seconds:** 0 (zero)

**OID:** eagleXgDiameterFsmOpStateUnavailable

**Recovery:**

1. 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.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 22102 - FsmOpStateDegraded

**Alarm Group:** DIAM

**Description:** Connection is only available for routing messages with a priority greater than or equal to the connection's congestion level.

**Severity:** Major

**Instance:** <Connection Name>

**HA Score:** Normal

**Auto Clear Seconds:** 0 (zero)

**OID:** eagleXgDiameterFsmOpStateDegraded

**Recovery:**

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

**22103 - SCTP Path Unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | SCTP multi-homed connection has operationally unavailable path. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | <ConnectionName>  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterSctpPathUnavailable                              |

**Recovery:**

1. The alarm will clear 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.

2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22104 - SCTPPathMismatch**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | SCTP multi-homed connection has path mismatch. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | <ConnectionName>                               |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                       |
| <b>OID:</b>                | eagleXgDiameterSctpPathMismatch                |

**Recovery:**

1. The alarm will clear when the connection is operationally unavailable.

Potential causes are:

- A host IP interface is down.
- A host IP interface is unreachable from the peer.
- The connection is misconfigured on the host.
- A peer IP interface is down.
- A peer IP interface is unreachable from the host.
- The connection is misconfigured on the peer.

2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 22200 - MpCpuCongested

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM                                     |
| <b>Description:</b>        | DA-MP CPU utilization threshold crossed. |
| <b>Severity:</b>           | Minor, Major, Critical                   |
| <b>Instance:</b>           | dSr.Cpu, ExgStack                        |
| <b>HA Score:</b>           | Normal                                   |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                 |
| <b>OID:</b>                | eagleXgDiameterMpCpuCongestedNotify      |

### 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, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 22201 - MpRxAllRate

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | DA-MP ingress message rate threshold crossed. |
| <b>Severity:</b>           | Minor, Major, Critical                        |
| <b>Instance:</b>           | MpRxAllRate, DIAM                             |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                      |
| <b>OID:</b>                | 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 \(MOS\)](#).

## 22202 - MpDiamMsgPoolCongested

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | DA-MP Diameter message pool utilization threshold crossed. |
| <b>Severity:</b>           | Minor, Major, Critical                                     |
| <b>Instance:</b>           | MpDiamMsgPool, DIAM  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#).

## 22203 - PTR Buffer Pool Utilization

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | DIAM  |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | Minor, Major, Critical  |

|                            |  |
|----------------------------|--|
| <b>Instance:</b>           | N/A                                    |
| <b>HA Score:</b>           | Normal                                 |
| <b>Auto Clear Seconds:</b> | 0 (zero)                               |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22204 - Request Message Queue Utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#).

## 22205 - Answer Message Queue Utilization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#).

## 22206 - Reroute Queue Utilization

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | DIAM  |
| <b>Description:</b> | 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. |

|                            |                                       |
|----------------------------|---------------------------------------|
| <b>Severity:</b>           | Minor, Major, Critical                |
| <b>Instance:</b>           | N/A                                   |
| <b>HA Score:</b>           | Normal                                |
| <b>Auto Clear Seconds:</b> | 0 (zero)                              |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22207 - DclTxTaskQueueCongested**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | DCL egress task message queue utilization threshold crossed. |
| <b>Severity:</b>           | Minor, Major, Critical                                       |
| <b>Instance:</b>           | <DA-MP Name>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22208 - DclTxConnQueueCongested**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | DCL egress connection message queue utilization threshold crossed. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <ConnectionName>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 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 \(MOS\)](#) 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 \(MOS\)](#).

## 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 \(MOS\)](#).

## 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 **Main Menu > 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 **Main Menu > 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 **Main Menu > 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 \(MOS\)](#).

## 22222 - Long Timeout PTR Buffer Pool Utilization

**Alarm Group:** DIAM

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | The MP's Long Timeout PTR buffer pool is approaching its maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 **Main Menu > 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 **Main Menu > 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 **Main Menu > 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 **Main Menu > Alarms & Events**.
6. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22223 - MpMemCongested**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | DA-MP memory utilization threshold crossed. |
| <b>Severity:</b>           | Minor, Major, Critical                      |
| <b>Instance:</b>           | System.RAM_UtilPct, DSR                     |
| <b>HA Score:</b>           | Normal                                      |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                    |
| <b>OID:</b>                | eagleXgDiameterMpMemCongestedNotify         |

**Recovery:**

Potential causes for this alarm are:

- One or more peers are generating more traffic than is nominally expected.
- Configuration requires more CPU usage for message processing than is nominally expected.
- One or more peers are answering slowly, causing a backlog of pending transactions.

**22224 - Average Hold Time Limit Exceeded**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | The average transaction hold time has exceeded its configured limits. |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterAvgHoldTimeLimitExceededNotify                         |

**Recovery:**

The average transaction hold time is exceeding its configured limits, resulting in an abnormally large number of outstanding transactions. Reduce the average hold time by examining the configured Pending Answer Timer values and reducing any values that are unnecessarily large.

**22225 - MpRxDiamAllLen**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | The Diameter average ingress message length threshold was crossed. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | <DA-MP Name>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterMpRxDiamAllLen                                      |

**Recovery:**

The alarm will clear when the average ingress message length falls below the clear threshold. The alarm may be caused by one or more peers generating larger messages than is nominally expected.

**22328 - IcRate**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | DIAM   |
| <b>Description:</b> | The diameter connection specified in the alarm instance is processing a higher than normal ingress messaging rate.   |
| <b>Severity:</b>    | <ul style="list-style-type: none"> <li>• Minor (if all of the following are true):           <ul style="list-style-type: none"> <li>• The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection minor alarm threshold.</li> </ul> </li> </ul> |

- The average ingress MPS rate that the connection is processing has not yet reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.
- Major (if the following are true):
  - The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

**Instance:** <Connection Name>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterImr

**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 that 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 that 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.

**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.

**Note:** The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu > Diameter > Configuration > System Options** screen.

**Severity:** Major, Critical

**Note:** The Critical threshold may be disabled by setting the Critical Threshold to zero using the "Alarm Threshold Options" tab on the **Main Menu > Diameter > Configuration > System Options** screen.

**Instance:** <NetworkElement>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterIPFEConnUnavailableThresholdReachedNotify

**Recovery:**

1. Use **Main Menu > Diameter > Maintenance > Connection** to monitor IPFE Connection status.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm that 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 that the peers in the Route List are not under maintenance.
5. It is recommended to contact [My Oracle Support \(MOS\)](#) 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 the **Main Menu > Diameter > Configuration > System Options** screen.  
**Severity:** Major, Critical  
**Note:** The Critical threshold may be disabled by setting the Critical Threshold to zero using the "Alarm Threshold Options" tab on the **Main Menu > Diameter > Configuration > System Options** screen.  
**Instance:** <DA-MP-Hostname>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterConnUnavailableThresholdReachedNotify

**Recovery:**

1. Use **Main Menu > Diameter > Maintenance > Connection** to monitor Fixed Connection status.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm that 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 that the peers in the Route List are not under maintenance.
5. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22900 - DPI DB Table Monitoring Overrun**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <DbTblName><br><br><b>Note:</b> <DbTblName> refers to the name of the Diameter Connection Status Sharing Table the Diameter Connection status inconsistency that was detected.   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterDpiTblMonCbOnLogOverrunNotify   |
| <b>Recovery:</b>         | It is recommended to contact <a href="#">My Oracle Support (MOS)</a> if this alarm is constantly being asserted and cleared.   |

**22901 - DPI DB Table Monitoring Error**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | An unexpected error occurred during DB Table Monitoring.               |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | DpiTblMonThreadName  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterDpiSldbMonAbnormalErrorNotify                           |
| <b>Recovery:</b>         | It is recommended to contact <a href="#">My Oracle Support (MOS)</a> . |

**22950 - Connection Status Inconsistency Exists**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | DIAM   |
| <b>Description:</b> | Diameter Connection status inconsistencies exist among the DA-MPs in the DSR signaling NE. |
| <b>Severity:</b>    | Critical   |

|                            |  |
|----------------------------|--|
| <b>Instance:</b>           | <DbTblName> (Name of the Diameter Connection Status Sharing Table where the Diameter Connection status inconsistency was detected) |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterConnStatusInconsistencyExistsNotify   |

**Recovery:**

No action necessary.

**Note:** DA-MP's SLDB tables are automatically audited and re-synchronized to correct inconsistencies after a log overrun has occurred.

**22960 - DA-MP Profile Not Assigned**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | A DA-MP configuration profile has not been assigned to this DA-MP. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterDaMpProfileNotAssignedNotify                        |

**Recovery:**

1. A DA-MP profile must be assigned to the DA-MP via the DSR OAM GUI.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22961 - Insufficient Memory for Feature Set**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | The Available Memory (in kilobytes) for Feature Set is less than the Required Memory (in kilobytes). |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 25607 - DSR Signaling Firewall is administratively Disabled

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | DSR Signaling Firewall is administratively Disabled |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | <System OAM name>                                   |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | N/A   |
| <b>OID</b>                | eagleXgDiameterFwDisabledNotify                     |

#### Recovery

1. Navigate to the Signaling Firewall page (**Main Menu > Diameter > Maintenance > Signaling Firewall**). Click the **Enable** button.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 25608 - Abnormal DA-MP Firewall

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DIAM   |
| <b>Description</b>        | DSR Signaling Firewall Operational status is degraded. |
| <b>Severity</b>           | Minor  |
| <b>Instance</b>           | <DA-MP name>   |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | N/A  |
| <b>OID</b>                | 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 (**Main Menu > Diameter > Maintenance > Signaling Firewall**).
4. If the alarm persists, restart the application on the identified DA-MP from the **Main Menu > Status & Manage** screen on the active Network OAM GUI.
5. If the problem is still unresolved, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 25609 - Firewall Configuration Error encountered

|                   |      |
|-------------------|------|
| <b>Event Type</b> | DIAM |
|-------------------|------|

|                         |  |
|-------------------------|--|
| <b>Description</b>      | Firewall Configuration Error encountered |
| <b>Severity</b>         | Info                                     |
| <b>Instance</b>         | <DA-MP name>                             |
| <b>HA Score</b>         | Normal                                   |
| <b>Throttle Seconds</b> | N/A                                      |
| <b>OID</b>              | eagleXgDiameterFwDisabledNotify          |

**Recovery**

This event is unexpected. Contact [My Oracle Support \(MOS\)](#) for analysis and resolution.

**25610 - DSR Signaling Firewall configuration inconsistency detected**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | DSR Signaling Firewall configuration inconsistency detected |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | <DA-MP name>  |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | N/A   |
| <b>OID</b>                | 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 \(MOS\)](#) for assistance.

**25805 - Invalid Shared TTG Reference**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | Invalid Shared TTG Reference                                  |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | <Route List Name>&<Route Group Name>&<TTG SG Name>&<TTG Name> |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | N/A   |
| <b>OID</b>                | 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,

- 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

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DIAM  |
| <b>Description</b>        | Invalid Internal SOAM Server Group Designation                |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | <Route List Name>&<Route Group Name>&<TTG SG Name>&<TTG Name> |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | N/A   |
| <b>OID</b>                | eagleXgDiameterDoicInvalidInternalSoamSgDesignationNotify     |

### Recovery

For the Route List named in the alarm instance, edit its configuration and delete the association to the Shared TTG. This will clear the alarm. The association can simply be re-added to restore integrity to the configuration.

## Range Based Address Resolution (RBAR) Alarms and Events (22400-22424)

### 22400 - Message Decoding Failure

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | RBAR   |
| <b>Description:</b>      | A message received was rejected because of a decoding failure. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterRbarMsgRejectedDecodingFailureNotify            |

### Recovery:

While parsing the message, the message content was inconsistent with the Message Length in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

### 22401 - Unknown Application ID

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | RBAR  |
| <b>Description:</b>      | A message could not be routed because the Diameter Application ID is not supported. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MPName>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterRbarUnknownAppIdNotify   |

#### 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

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | RBAR   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | RBAR   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <AddressResolution>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | RBAR  |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <AddressResolution>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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**

|                    |      |
|--------------------|------|
| <b>Event Type:</b> | RBAR |
|--------------------|------|

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <AddressResolution>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | RBAR   |
| <b>Description:</b>      | 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 <a href="#">22200 - MpCpuCongested</a> . |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterRbarRoutingAttemptFailureInternalResExhNotify   |

**Recovery:**

If this problem occurs, it is recommended to contact [My Oracle Support \(MOS\)](#).

**22407 - Routing attempt failed due to internal database inconsistency failure**

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | RBAR  |
| <b>Description:</b> | A message could not be routed because an internal address resolution run-time database inconsistency was encountered. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | <MPName>  |

|                          |  |
|--------------------------|--|
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterRbarRoutingFailureInternalDbInconsistencyNotify |

**Recovery:**

If this problem occurs, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 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

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | APPL   |
| <b>Description:</b>        | DSR Application is unable to process any messages because it is Unavailable.   |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | <DSR Application Name><br><br><b>Note:</b> The value for DSR Application Name will vary 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. |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterDsrApplicationUnavailableNotify   |

**Recovery:**

1. Display and monitor the DSR Application status by selecting **Diameter > Maintenance > Applications** in the SO GUI. Verify that 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 **Main Menu > 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 will 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 \(MOS\)](#).

**22501 - DSR Application Degraded**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | APPL  |
| <b>Description:</b>        | Unable to forward requests to the DSR Application because it is Degraded.   |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | <DSR Application Name><br><br><b>Note:</b> The value for DSR Application Name will vary 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. |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterDsrApplicationDegradedNotify   |

**Recovery:**

1. Display and monitor the DSR Application status by selecting **Diameter > Maintenance > Applications** in the SO GUI. Verify that the Admin State is set as expected.
2. A DSR Application becomes Degraded when the DSR Application becomes congested if enabled.  
  
**Note:** This alarm will NOT be raised when the DSR application is shutting down gracefully or application is in Disabled state. Only the DSR Application operational status will be 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 \(MOS\)](#).

**22502 - DSR Application Request Message Queue Utilization**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | APPL  |
| <b>Description:</b> | The DSR Application Request Message Queue Utilization is approaching its maximum capacity.  |
| <b>Severity:</b>    | Minor, Major, Critical  |
| <b>Instance:</b>    | <Metric ID>, <DSR Application Name><br><br><b>Note:</b> The value for Metric ID for this alarm will vary (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.<br><br><b>Note:</b> 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 that 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**.
3. 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 Request Message Queue. Examine the Alarm log in **Alarms & Events**
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**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 will vary (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 DSR Application Name will vary 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**
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 22504 - DSR Application Ingress Message Rate

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | APPL  |
| <b>Description:</b>        | The ingress message rate for the DSR Application is exceeding its engineered traffic handling capacity.   |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | <Metric ID>, <DSR Application Name>   |
|                            | <p><b>Note:</b> The value for Metric ID for this alarm will vary (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.</p> <p><b>Note:</b> The value for DSR Application Name will vary 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.</p> |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterDsrApplicationIngressMsgRateNotify   |

### 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. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu > Status & Manage > KPIs**.  
If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 22520 - DSR Application Enabled

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | APPL  |
| <b>Description:</b>      | DSR Application Admin state was changed to 'enabled'.   |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <DSR Application Name>, the DCA App short name ( <i>DcaDalld.shortName</i> ) prefixed with "DCA:" |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |

**OID:** eagleXgDiameterDsrApplicationEnabledNotify

**Recovery:**  
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 (*DcaDalld.shortName*) prefixed with "DCA:"  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** eagleXgDiameterDsrApplicationDisabledNotify

**Recovery:**  
No action required.

## Full Address Based Resolution (FABR) Alarms and Events (22600-22640)

### 22600 - Message Decoding Failure

**Event Type:** FABR  
**Description:** Message received was rejected because of a decoding failure. While parsing the message, the message content was inconsistent with the "Message Length" in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message), the peer who forwarded the message to this node, or any intermediate node that modifies the message.  
**Severity:** Info  
**Instance:** <MPName>  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterFabrMsgRejectedDecodingFailureNotify

**Recovery:**  
It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22601 - Unknown Application ID**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | FABR   |
| <b>Description:</b>      | <p>Message could not be routed because the Diameter Application ID is not supported.</p> <p>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.</p> |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterFabrUnknownAppIdNotify  |

**Recovery:**

1. The currently provisioned Application Routing Rules can be viewed using **Main Menu > Diameter > Configuration > Application Route Tables**.
2. The currently provisioned Diameter Application IDs can be viewed in the **FABR > Configuration > Applications Configuration**.
3. Contact [My Oracle Support \(MOS\)](#) for assistance.

**22602 - Unknown Command Code**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | FABR   |
| <b>Description:</b>      | <p>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.</p> <p>Either an application routing rule is mis-provisioned or the Command Code is not provisioned in the FABR configuration.</p> |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterFabrUnknownCmdCodeNotify  |

**Recovery:**

1. The currently provisioned Application Routing Rules can be viewed using **Main Menu > 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 \(MOS\)](#) for assistance.

### 22603 - No Routing Entity Address AVPs

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | FABR   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <AddrResolution>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 **Main Menu > Diameter > Configuration > Application Route Tables**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 22604 - No valid User Identity Addresses found

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | FABR   |
| <b>Description:</b>      | No valid User Identity Address is found in the configured AVPs contained in the ingress message. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <AddrResolution>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterFabrNoValidUserIdentityAddrFoundNotify  |

#### 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 **Main Menu > Diameter > Configuration > Application Route Tables**.
3. Contact [My Oracle Support \(MOS\)](#) for assistance.

### 22605 - No Destination address is found to match the valid User Identity address

|                    |      |
|--------------------|------|
| <b>Event Type:</b> | 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 \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

## 22607 - Routing attempt failed due to DRL queue exhaustion

**Event Type:** FABR

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | Message could not be routed because the internal "Request Message Queue" to the DSR Relay Agent was full. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MPNname>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterFabrRoutingAttemptFailureDrIQueueExhNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22608 - Database query could not be sent due to DB congestion**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | FABR   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <MPNname>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterFabrDpCongestedNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22609 - Database connection exhausted**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | FABR  |
| <b>Description:</b>      | Database queries could not be sent because the database connection (ComAgent) queue was full. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MPNname>   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterFabrDbConnectionExhNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22610 - FABR DP Service congestion state change**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | FABR  |
| <b>Description:</b>      | FABR application received status notification indicating DP congestion state change or DP congestion abatement time period has completed. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <MPName>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |
| <b>OID:</b>              | eagleXgDiameterFabrDpCongestionStateChangeNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22611 - FABR Blacklisted Subscriber**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | FABR   |
| <b>Description:</b>      | Message could not be routed because valid User Identity Address extracted from diameter request belongs to blacklisted subscriber. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <AddrResolution>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 \(MOS\)](#).

**22631 - FABR DP Response Task Message Queue Utilization**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | FABR  |
| <b>Description:</b> | The FABR Application's DP Response Message Queue Utilization is approaching its maximum capacity. |
| <b>Severity:</b>    | Minor, Major, Critical  |
| <b>Instance:</b>    | 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 \(MOS\)](#) for assistance.

**22632 - COM Agent Registration Failure**

**Alarm Group:** FABR  
**Description:** The Communication Agent routing service registration or service notification registration failed, FABR can not use the Communication Agent service for database queries.  
**Severity:** Critical  
**Instance:** Full Address Based Resolution  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterComAgentRegistFailNotify

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22701 - Protocol Error in Diameter Answers**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | PCA  |
| <b>Description:</b>      | The Diameter Answer message(s) received by PCA contain(s) protocol error(s). This error message is based on error scenarios such as: <ul style="list-style-type: none"> <li>• Command-Code value is not supported</li> <li>• Mandatory AVP used for processing decisions is missing</li> <li>• Mandatory AVP used for processing contains an invalid value</li> <li>• Mandatory Session-Id AVP has a zero-length value</li> </ul> <p><b>Note:</b> 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.</p> |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | PCA, <PcaFunctionName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | pdraPdraProtocolErrorsInDiameterAnsNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22702 - Database Hash Function Error**

|                     |   |
|---------------------|---|
| <b>Event Type:</b>  | PCA   |
| <b>Description:</b> | The hash function result does not map to a database resource or sub-resource. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | N/A   |
| <b>HA Score:</b>    | Normal  |
| <b>OID:</b>         | pdraPdraHashingResDoesNotMatchResOrSubResNotify                               |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22703 - Diameter Message Routing Failure Due To Full DRL Queue**

|                     |  |
|---------------------|--|
| <b>Event Type:</b>  | PCA  |
| <b>Description:</b> | The Diameter Egress message could not be sent because the DRL Message Queue is full. |
| <b>Severity:</b>    | 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 \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22706 - Binding Key Not Found In Diameter Message**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | PCA   |
| <b>Description:</b>      | A binding key is not found in the received CCR-I message. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | pdraPdraBindingKeyNotFoundNotify                          |

**Recovery:**

1. Check the P-DRA GUI at **Policy DRA > Configuration > Binding Key Priority**.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance

**22707 - Diameter Message Processing Failure**

|                          |  |
|--------------------------|--|
| <b>Alarm Group:</b>      | PCA  |
| <b>Description:</b>      | PCA failed to process a Diameter message. The specific reason is provided by the PCA signaling code. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <PcaFunctionName>  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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 \(MOS\)](#) for further assistance.

**22708 - PCA Function is Disabled**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PCA  |
| <b>Description:</b>        | The PCA Function is unable to process any messages because it is Disabled. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <PcaFunctionName>  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 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 **Main Menu > 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 (MOS)* 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 \(MOS\)](#) for assistance if needed.

## 22710 - SBR Sessions Threshold Exceeded

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SBR   |
| <b>Description:</b>        | The number of SBR sessions threshold for a Policy and Charging Mated Sites Place Association has been exceeded. |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | <SbrDatabaseName>   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterPSbrActSessThreshNotify  |

### Recovery:

1. The session database specified in the Instance field is nearing the limit on the number of session records. The alarm thresholds for Session Capacity alarms are configured network wide on the Network OAM from the **Policy and Charging > Configuration > Alarm Settings** screen. 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 from the Network OAM Gui Main menu from **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 \(MOS\)](#) for further assistance.

## 22711 - SBR Database Error

|                          |  |
|--------------------------|--|
| <b>Alarm Group:</b>      | SBR  |
| <b>Description:</b>      | An error occurred during a SBR database operation. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <SbrServerType>, <SbrSgNameDbType> (I-SBR)         |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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:
  1. The database is filled to capacity
  2. 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 \(MOS\)](#) for further assistance.

**22712 - SBR Communication Error**

|                          |  |
|--------------------------|--|
| <b>Alarm Group:</b>      | SBR  |
| <b>Description:</b>      | The SBR received an error or timeout response from Communication Agent when sending a stack event to another SBR server. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <SbrServerType>, <SbrDbType> (I-SBR)   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | eagleXgDiameterPSBRStkEvFailComAgentNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**22713 - SBR Alternate Key Creation Error**

|                          |   |
|--------------------------|---|
| <b>Alarm Group:</b>      | SBR   |
| <b>Description:</b>      | Failed to create an Alternate Key record in the Binding database. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Session SBR   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | eagleXgDiameterPSBRAltKeyCreateFailNotify                         |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**22714 - SBR RAR Initiation Error**

|                     |     |
|---------------------|-----|
| <b>Alarm Group:</b> | SBR |
|---------------------|-----|

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | SBR encountered an error while processing PCA initiated RAR requests. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Session SBR   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | eagleXgDiameterPSBRRARInitiationErrNotify                             |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**22715 - SBR Audit Suspended**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SBR   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22716 - SBR Audit Statistics Report**

|                     |  |
|---------------------|--|
| <b>Event Group:</b> | SBR  |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | Info   |

**Instance:** <PcaTableName>, <SbrSgName> (I-SBR)  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** eagleXgDiameterPSBRAuditStatisticsReportNotify

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**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:**

If the further assistance is needed, it is recommended to contact [My Oracle Support \(MOS\)](#).

**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

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | A Binding capable session initiation request failed because this subscriber already has the maximum number of sessions per binding. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | N/A   |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | 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 \(MOS\)](#).

**22720 - Policy SBR To PCA Response Queue Utilization Threshold Exceeded**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PCA  |
| <b>Description:</b>        | The SBR to PCA Response Queue Utilization Threshold Exceeded |
| <b>Severity:</b>           | Minor, Major, Critical                                       |
| <b>Instance:</b>           | RxPcaSbrEventMsgQueue, PCA                                   |
| <b>HA Score:</b>           | Normal   |
| <b>OID:</b>                | pdraPdraPsbrResponseQueueUtilizationNotify                   |
| <b>Auto Clear Seconds:</b> | 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 **Main Menu > 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 **Main Menu > 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 **Main Menu > 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 \(MOS\)](#).

**22721 - Policy and Charging Server In Congestion**

|                     |     |
|---------------------|-----|
| <b>Alarm Group:</b> | PCA |
|---------------------|-----|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | The Policy and Charging Server is operating in congestion. |
| <b>Severity:</b>           | Minor, Major, Critical                                     |
| <b>Instance:</b>           | PCA  |
| <b>HA Score:</b>           | Normal   |
| <b>OID:</b>                | pdraPdraCongestionStateNotify                              |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |

**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 **Main Menu > 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 \(MOS\)](#).

**22722 - Policy Binding Sub-resource Unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PCA   |
| <b>Description:</b>        | One or more Policy binding sub-resources are not available.   |
| <b>Severity:</b>           | <ul style="list-style-type: none"> <li>• 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</li> <li>• 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.</li> </ul> |
| <b>Instance:</b>           | <ResourceDomainName>  |
| <b>HA Score:</b>           | Normal  |
| <b>OID:</b>                | pdraPdraBindingSubresourceUnavailableNotify   |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |

**Recovery:**

1. At the NOAM, navigate to the SBR Database Status screen at **Main Menu > 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:

- **Main Menu > Configuration > Resource Domains**
  - **Main Menu > Configuration > Places**
  - **Main Menu > 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 **Main Menu > 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 \(MOS\)](#) for assistance if needed.

## 22723 - Policy and Charging Session Sub-resource Unavailable

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PCA   |
| <b>Description:</b>        | One or more Policy and Charging session sub-resources are not available.  |
| <b>Severity:</b>           | <ul style="list-style-type: none"> <li>• 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.</li> <li>• Critical: When a Session SBR Database is prepared or enabled and all of the server groups hosting session sub-resources are not available.</li> </ul> |
| <b>Instance:</b>           | <ResourceDomainName>  |
| <b>HA Score:</b>           | Normal  |
| <b>OID:</b>                | pdraPdraSessionSubresourceUnavailableNotify   |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |

### Recovery:

1. At the NOAM, navigate to the SBR Database Status screen at **Main Menu > 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:

- **Main Menu > Configuration > Resource Domains**
  - **Main Menu > Configuration > Places**
  - **Main Menu > 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 **Main Menu > 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 \(MOS\)](#) for assistance if needed.

## 22724 - SBR Memory Utilization Threshold Exceeded

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SBR  |
| <b>Description:</b>        | The SBR server memory utilization threshold has been exceeded. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | psbr.MemPerTotal, SBR  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterPSbrMemUtilNotify                               |

### Recovery:

1. If this condition persists, it may be necessary to allocate more memory for SBR.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

## 22725 - SBR Server In Congestion

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SBR  |
| <b>Description:</b>        | The SBR server is operating in congestion.   |
| <b>Severity:</b>           | <ul style="list-style-type: none"> <li>• Minor: CL_1</li> <li>• Major: CL_2</li> <li>• Critical: CL_3</li> </ul> |
| <b>Instance:</b>           | Policy and Charging mated Sites Place Association Name, <SbrSgName> (I-SBR)                                      |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 **Main Menu > 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 \(MOS\)](#).

**22726 - SBR Queue Utilization Threshold Exceeded**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SBR  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | SBR, <SbrQueueName> (I-SBR)  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterPSbrStackEvQUtilNotify  |

**Recovery:**

1. If this condition persists, it may be necessary to allocate larger queue sizes.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**22727 - SBR Initialization Failure**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SBR  |
| <b>Description:</b>        | The SBR server process failed to initialize.               |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | Policy DRA Mated Sites Place Association Name, N/A (I-SBR) |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterPSbrInitializationFailureNotify             |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**22728 - SBR Bindings Threshold Exceeded**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SBR   |
| <b>Description:</b>        | The number of bindings threshold has been exceeded. |
| <b>Severity:</b>           | Minor, Major, Critical                              |
| <b>Instance:</b>           | <SbrDatabaseName>                                   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) to discuss plans for system growth if 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**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PCA  |
| <b>Description:</b>        | PCRF Not Configured                          |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | Policy Binding Region Place Association Name |
| <b>HA Score:</b>           | Normal                                       |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                     |
| <b>OID:</b>                | pdraPcrfNotConfiguredNotify                  |

**Recovery:**

1. Check the NOAM GUI at **Main Menu > 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 \(MOS\)](#).

**22730 - Policy and Charging Configuration Error**

|                     |     |
|---------------------|-----|
| <b>Alarm Group:</b> | PCA |
|---------------------|-----|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | Policy and Charging message processing could not be successfully completed due to a configuration error. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | <ConfigurationError>   |
| <b>HA Score:</b>           | Normal   |
| <b>OID:</b>                | pdraPdraConfigErrorNotify  |
| <b>Auto Clear Seconds:</b> | 300 (5 minutes)  |

**Recovery:**

1. If there is an unconfigured PCRF, it means that 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 that 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 that included the OCS.
6. It is recommended to contact [My Oracle Support \(MOS\)](#)

**22731 - Policy and Charging Database Inconsistency**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PCA   |
| <b>Description:</b> | The Policy and Charging database inconsistency exists due to an internal data error or internal database table error. |
| <b>Severity:</b>    | Major   |
| <b>Instance:</b>    | <PcaFunctionName>   |

|                            |                                     |
|----------------------------|-------------------------------------|
| <b>HA Score:</b>           | Normal                              |
| <b>Auto Clear Seconds:</b> | 60                                  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22732 - SBR Process CPU Utilization Threshold Exceeded**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | SBR  |
| <b>Description:</b>        | The SBR process on the indicated server is using higher than expected CPU resources. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | psbr.cpu, SBR  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for further assistance.

**22733 - SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SBR   |
| <b>Description:</b>        | The SBR failed to free binding memory after PCRF Pooling binding migration. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | N/A   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**22734 - Policy and Charging Unexpected Stack Event Version**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PCA  |
| <b>Description:</b>        | A Policy and Charging server received a stack event with an unexpected down-version. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>OID:</b>                | pdraPdraUnexpectedSEDownVersionNotify  |
| <b>Auto Clear Seconds:</b> | 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 \(MOS\)](#).

**22735 - Policy DRA session initiation request received with no APN**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | PDRA  |
| <b>Description:</b>      | A Policy DRA session initiation request was received with no APN. |
| <b>Severity:</b>         | Info  |
| <b>HA Score:</b>         | Normal  |
| <b>Instance:</b>         | None  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | 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 \(MOS\)](#).

### 22736 - SBR failed to free shared memory after a PCA function is disabled

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SBR   |
| <b>Description:</b>        | SBR failed to free shared memory after a PCA function is disabled |
| <b>Severity:</b>           | Minor   |
| <b>HA Score:</b>           | Normal  |
| <b>Instance:</b>           | <PcaFunctionName>   |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | pdraPSBRPostPcaFunctionDisableMemFreeNotify                       |

**Recovery:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 22737 - Configuration Database Not Synced

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PCA   |
| <b>Description:</b>        | Configuration Database is not synced between the System OAM and Network OAMP. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | Site name of SOAM server which asserted this alarm                            |
| <b>HA Score:</b>           | Normal  |
| <b>OID:</b>                | pdraPcaConfDbNotSyncedNotify  |
| <b>Auto Clear Seconds:</b> | 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 \(MOS\)](#).

### 22738 - SBR Database Reconfiguration State Transition

|                     |  |
|---------------------|--|
| <b>Event Group:</b> | SBR  |
| <b>Description:</b> | 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.

|                          |   |
|--------------------------|---|
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <SbrReconfigurationPlanName>, <SbrReconfigurationPlanName><br>(I-SBR) |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |
| <b>OID:</b>              | eagleXgDiameterPsbrReconfigStateTransitionNotify                      |

**Recovery:**

This event records the time and conditions under which an SBR Database Reconfiguration Plan (identified in the event instance field) undergoes a state transition. The event additional information includes details such as the previous state, current state, and whether the "Force" option was chosen. This event can be used to obtain a timeline of the entire history of a given reconfiguration plan.

**22740 - SBR Reconfiguration Plan Completion Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SBR   |
| <b>Description:</b>        | Failed to successfully complete an SBR Reconfiguration Plan.<br><br><b>Note:</b> When an SBR Reconfiguration Plan is completed by the user clicking <b>Complete</b> , or <b>Force Complete</b> 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. <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• Condition 3: Failed to mark the Target SBR Database as the default database for the Place Association on completion of a Data Migration Plan.</li> <li>• Condition 4: Failed to enable the Target SBR Database on completion of a Data Migration Plan.</li> <li>• Condition 5: Failed to disable the Initial SBR Database on completion of a Data Migration Plan.</li> </ul> |
| <b>Severity:</b>           | <ul style="list-style-type: none"> <li>• Minor: Condition 5</li> <li>• Critical: Conditions 1-4</li> </ul>  |
| <b>Instance:</b>           | <SbrReconfigPlanAndCondition>   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterPSbrReconfigConditionsErrorNotify  |

**Recovery:**

The SBR Reconfiguration plan specified in the Alarm Instance was not successfully completed, possibly leaving the SBR Database in an abnormal state. Make note of the specific reason for the alarm, and it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**22741 - Failed to route PCA generated RAR**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | PCA  |
| <b>Description:</b>      | Unable to Route RAR generated at PCA         |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | N/A  |
| <b>HA Score:</b>         | Normal                                       |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | eagleXgDiameterPcaGeneratedRARRouteErrNotify |

**Recovery:**

Use Destination-Host to identify the locally generated RAR routing failures and correct the respective configurations. If the DRL provides an error message, it will be displayed with this event, which will have a 3-digit internal error code.

**22750 - Enhanced Suspect Binding Removal Feature Enabled**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | SBR  |
| <b>Description:</b>      | The Enhanced Suspect Binding Feature is enabled. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | N/A  |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 0 (zero)   |
| <b>OID:</b>              | eagleXgDiameterEnhSuspBindingFeatEnabledNotify   |

**Recovery:**

No action required.

**22751 - Binding Audit Suppression by Suspect Binding Removal**

**Alarm Group:** SBR

**Description:** The binding SBR audit function is suppressed by the Enhanced Suspect Binding Removal feature.

**Severity:** Minor

**Instance:** PCA

**HA Score:** Normal

**Auto Clear Seconds:** 0 (zero)

**OID:** eagleXgDiameterEnhSuspectBindingAuditSuppressionNotify

**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 \(MOS\)](#) 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

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | TVOE  |
| <b>Description:</b>        | This alarm indicates that the libvirtd daemon is not running. |
| <b>Severity:</b>           | Major   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 1.3.6.1.4.1.323.5.3.31.1.1.2.1                                |
| <b>Alarm ID:</b>           | TKSTVOEMA1  |

**Recovery:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 24401 - TVOE libvirtd is hung

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | TVOE  |
| <b>Description:</b>        | This alarm indicates that we attempted to determine if the libvirtd daemon is not responding and it didn't respond. |
| <b>Severity:</b>           | Major   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 1.3.6.1.4.1.323.5.3.31.1.1.2.2  |
| <b>Alarm ID:</b>           | TKSTVOEMA2  |

**Recovery:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 24402 - all TVOE libvirtd connections are in use

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | TVOE  |
| <b>Description:</b>        | This alarm indicates that all twenty connections to libvirtd are in use and more could be killed. |
| <b>Severity:</b>           | Major   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 1.3.6.1.4.1.323.5.3.31.1.1.2.3  |
| <b>Alarm ID:</b>           | TKSTVOEMA3  |

#### Recovery:

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

## 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

|                            |  |
|----------------------------|--|
| <b>Event Type:</b>         | CAPM   |
| <b>Description:</b>        | <p>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.</p> <p>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.</p> |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | <ruleset> or <ruleset:rule-id>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | CAPM  |
| <b>Description:</b>      | When a new Rule Template is created, a failure occurs when performing the action. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <ruleset> or <ruleset:rule-id>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | eagleXgDiameterCapmActionFailedNotify   |

**Recovery:**

Check the reasons the action failed. It may be a lack of system resources to perform an action, or the action may refer to a part of the message that is not available.

**25002 - CAPM Exit Rule Template**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | CAPM  |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <ruleset> or <ruleset:rule-id>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | eagleXgDiameterCapmExitRuleFailedNotify   |

**Recovery:**

No action required.

**25003 - CAPM Exit Trigger**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | CAPM   |
| <b>Description:</b>      | 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). |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <ruleset> or <ruleset:rule-id>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 30   |
| <b>OID:</b>              | eagleXgDiameterCapmExitTriggerFailedNotify   |
| <b>Recovery:</b>         | No action required.  |

**25004 - Script failed to load**

|                            |  |
|----------------------------|--|
| <b>Alarm Type:</b>         | CAPM   |
| <b>Description:</b>        | Script syntax error                          |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | <script name>                                |
| <b>HA Score:</b>           | Normal                                       |
| <b>Auto Clear Seconds:</b> | 0 (zero)                                     |
| <b>OID:</b>                | eagleXgDiameterCapmScriptLoadingFailedNotify |
| <b>Recovery:</b>           | Check for syntax errors in the script        |

**25005 - CAPM Generic Event**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | CAPM                                      |
| <b>Description:</b>      | CAPM Generic Event                        |
| <b>Severity:</b>         | Info                                      |
| <b>Instance:</b>         | <template-id:rule-id>                     |
| <b>HA Score:</b>         | Normal                                    |
| <b>Throttle Seconds:</b> | 30  |
| <b>OID:</b>              | eagleXgDiameterCapmGenericInfoAlarmNotify |
| <b>Recovery:</b>         |   |

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 25006 - CAPM Generic Alarm - Minor

|                            |  |
|----------------------------|--|
| <b>Event Type:</b>         | CAPM                                       |
| <b>Description:</b>        | CAPM Generic Alarm - Minor                 |
| <b>Severity:</b>           | Minor                                      |
| <b>Instance:</b>           | <template-id:rule-id>                      |
| <b>HA Score:</b>           | Normal                                     |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | eagleXgDiameterCapmGenericMinorAlarmNotify |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 25007 - CAPM Generic Alarm - Major

|                            |  |
|----------------------------|--|
| <b>Event Type:</b>         | CAPM                                       |
| <b>Description:</b>        | CAPM Generic Alarm - Major                 |
| <b>Severity:</b>           | Major                                      |
| <b>Instance:</b>           | <template-id:rule-id>                      |
| <b>HA Score:</b>           | Normal                                     |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | eagleXgDiameterCapmGenericMajorAlarmNotify |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 25008 - CAPM Generic Alarm - Critical

|                            |   |
|----------------------------|---|
| <b>Event Type:</b>         | CAPM  |
| <b>Description:</b>        | CAPM Generic Alarm - Critical                 |
| <b>Severity:</b>           | Critical                                      |
| <b>Instance:</b>           | <template-id:rule-id>                         |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | eagleXgDiameterCapmGenericCriticalAlarmNotify |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

## 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

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | This alarm occurs when no active DA-MP leaders have been detected. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | <NetworkElement>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterNoDaMpLeaderDetectedNotify                          |

**Recovery:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 25510 - Multiple DA-MP Leader Detected Alarm

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIAM   |
| <b>Description:</b>        | This alarm occurs when multiple active DA-MP leaders have been detected. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | <NetworkElement>   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterMultipleDaMpLeadersDetectedNotify                         |

**Recovery:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**25800 - Peer Discovery Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIAM  |
| <b>Description:</b>        | Peer discovery failure.   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has failed. |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

**25801 - Peer Discovery Configuration Error Encountered**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | Peer discovery configuration error encountered.  |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has encountered a configuration error. |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 0 (zero)   |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance.

**25802 - Realm Expiration Approaching**

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | DIAM |
|---------------------|------|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | Realm expiration approaching.  |
| <b>Severity:</b>           | Minor, Major   |
| <b>Instance:</b>           | Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose expiry is approaching. |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

**25803 - Peer Discovery - Inconsistent Remote Host Port Assignment**

|                          |   |
|--------------------------|---|
| <b>Event Type:</b>       | DIAM  |
| <b>Description:</b>      | Peer discovery - inconsistent remote host port assignment.  |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has encountered inconsistent remote host port assignment. |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 0 (zero)  |
| <b>OID:</b>              | eagleXgDiameterDpdInconsistentPortAssignmentNotify  |

**Recovery:**

No action required. The DNS records for the Realm being discovered must be corrected by the Realm's DNS administrator.

**25804 - Peer Discovery State Change**

|                          |  |
|--------------------------|--|
| <b>Event Type:</b>       | DIAM   |
| <b>Description:</b>      | Peer discovery state change.   |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery state has changed. |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 0 (zero)   |

**OID:** eagleXgDiameterDpdInconsistentPortAssignmentNotify

**Recovery:**  
No action required.

## Platform (31000-32800)

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32800.

### 31000 - S/W fault

**Alarm Group:** SW

**Description:** Program impaired by s/w fault

**Severity:** Minor

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

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** comcolSwFaultNotify

**Recovery:**  
No action is required. This event is used for command-line tool errors only.

### 31001 - S/W status

**Alarm Group:** SW

**Description:** Program status

**Severity:** Info

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

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** comcolSwStatusNotify

**Recovery:**  
No action required.

**31002 - Process watchdog failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | Process watchdog timed out.   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31003 - Tab thread watchdog failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | Tab thread watchdog timed out   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolThreadWatchdogFailureNotify   |

**Recovery:**

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

**31100 - Database replication fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The Database replication process is impaired by a s/w fault                             |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |

**OID:** comcolDbReplicationFaultNotify

**Recovery:**

1. Export event history for the given server and inetsync task.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

### 31101 - Database replication to slave failure

**Alarm Group:** REPL

**Description:** Database replication to a slave Database has failed

**Severity:** Critical

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

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** comcolDbRepToSlaveFailureNotify

**Recovery:**

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact [My Oracle Support \(MOS\)](#).

### 31102 - Database replication from master failure

**Alarm Group:** REPL

**Description:** Database replication from a master Database has failed.

**Severity:** Minor

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

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** comcolDbRepFromMasterFailureNotify

**Recovery:**

1. 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.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 31103 - DB Replication update fault

**Alarm Group:** REPL

|                            |   |
|----------------------------|---|
| <b>Description:</b>        | Database replication process cannot apply update to DB.                                 |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31104 - DB Replication latency over threshold**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | Database replication latency has exceeded thresholds                                    |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31105 - Database merge fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The database merge process (inetmerge) is impaired by a s/w fault                       |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 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 \(MOS\)](#).

### 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 \(MOS\)](#).

### 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 \(MOS\)](#).

**31108 - Database merge latency over threshold**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | COLL  |
| <b>Description:</b>        | Database Merge latency has exceeded thresholds  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31109 - Topology config error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DB  |
| <b>Description:</b>        | Topology is configured incorrectly  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31110 - Database audit fault**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | SW  |
| <b>Description:</b> | The Database service process (idbsvc) is impaired by a s/w fault. |
| <b>Severity:</b>    | Minor   |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31111 - Database merge audit in progress**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | COLL  |
| <b>Description:</b>        | Database Merge Audit between mate nodes in progress                                     |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolDbMergeAuditNotify  |

**Recovery:**

No action required.

**31112 - DB replication update log transfer timed out**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | DB Replicated data may not have transferred in the time allotted.                       |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 30  |
| <b>OID:</b>                | comcolDbRepUpLogTransTimeoutNotify  |

**Recovery:**

1. No action required.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) if this occurs frequently.

**31113 - DB replication manually disabled**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | DB Replication Manually Disabled  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | comcolDbReplicationManuallyDisabledNotify   |
| <b>Recovery:</b>           | No action required.   |

**31114 - DB replication over SOAP has failed**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | REPL   |
| <b>Description:</b>        | Database replication of configuration data via SOAP has failed.  |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 3600   |
| <b>OID:</b>                | comcolDbReplicationSoapFaultNotify   |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>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.</li> <li>2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a>.</li> </ol> |

**31115 - Database service fault**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | SW  |
| <b>Description:</b> | The Database service process (idbsvc) is impaired by a s/w fault.                       |
| <b>Severity:</b>    | Minor   |
| <b>Instance:</b>    | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>    | 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 \(MOS\)](#).

**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:**

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 \(MOS\)](#).

**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 \(MOS\)](#).

**31118 - Database disk store fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DISK  |
| <b>Description:</b>        | Writing the database to disk failed   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31119 - Database updatelog overrun**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DB  |
| <b>Description:</b>        | The Database update log was overrun increasing risk of data loss                        |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31120 - Database updatelog write fault**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | DB  |
| <b>Description:</b> | A Database change cannot be stored in the updatelog                                     |
| <b>Severity:</b>    | Minor   |
| <b>Instance:</b>    | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |

|                            |                                   |
|----------------------------|-----------------------------------|
| <b>HA Score:</b>           | Normal                            |
| <b>Auto Clear Seconds:</b> | 300                               |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31121 - Low disk free early warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DISK  |
| <b>Description:</b>        | The amount of free disk is below configured early warning thresholds                    |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31122 - Excessive shared memory early warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | MEM   |
| <b>Description:</b>        | The amount of shared memory consumed exceeds configured early warning thresholds        |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31123 - Database replication audit command complete**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | ADIC found one or more errors that are not automatically fixable.                       |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolDbRepAuditCmdCompleteNotify   |
| <b>Recovery:</b>           | No action required.   |

**31124 - ADIC error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | An ADIC detected errors   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolDbRepAuditCmdErrNotify  |
| <b>Recovery:</b>           | It is recommended to contact <a href="#">My Oracle Support (MOS)</a> .                  |

**31125 - Database durability degraded**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | Database durability has dropped below configured durability level                       |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31126 - Audit blocked**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | REPL   |
| <b>Description:</b>        | Site Audit Controls blocked an inter-site replication audit due to the number in progress per configuration. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                      |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | comcolAuditBlockedNotify   |

**Recovery:**

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

**31127 - DB Replication Audit Complete**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | DB replication audit completed  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolDbRepAuditCompleteNotify  |

**Recovery:**

No action required.

**31128 - ADIC Found Error**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | REPL  |
| <b>Description:</b> | ADIC found one or more errors that are not automatically fixable. |
| <b>Severity:</b>    | Major   |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31129 - ADIC Found Minor Issue**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | REPL  |
| <b>Description:</b>        | ADIC found one or more minor issues that can most likely be ignored                     |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 14400   |
| <b>OID:</b>                | comcolDbADICWarn  |

**Recovery:**

No action required.

**31130 - Network health warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | NET   |
| <b>Description:</b>        | Network health issue detected   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31131 - DB Ousted Throttle Behind**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DB  |
| <b>Description:</b>        | DB ousted throttle may be affecting processes.  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 'procshn -o' to identify involved processes.
3. It is recommended to contact [My Oracle Support \(MOS\)](#).

**31132 - DB Replication Precedence Relaxed**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | REPL  |
| <b>Description</b>      | Standby Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Databases to update as fast as possible. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | Remote Node Name + HA resource name (if Policy 0, no resource name)   |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 150   |
| <b>OID</b>              | comcolDbRepPrecRelaxedNotify  |

**Recovery**

No action required.

**31133 - DB Replication Switchover Exceeds Threshold**

|                    |   |
|--------------------|---|
| <b>Alarm Group</b> | REPL  |
| <b>Description</b> | DB Replication Active to Standby switchover exceeded maximum switchover time. |
| <b>Severity</b>    | Major   |
| <b>Instance</b>    | Remote Node Name + HA resource name (if Policy 0, no resource name)           |

|                           |                             |
|---------------------------|-----------------------------|
| <b>HA Score</b>           | Normal                      |
| <b>Auto Clear Seconds</b> | 300                         |
| <b>OID</b>                | 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 \(MOS\)](#).

**31134 - DB Site Replication To Slave Failure**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | REPL  |
| <b>Description</b>        | DB Site replication to a slave DB has failed.                       |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | Remote Node Name + HA resource name (if Policy 0, no resource name) |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 300   |
| <b>OID</b>                | 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 \(MOS\)](#).

**31135 - DB Site Replication From Master Failure**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | REPL  |
| <b>Description</b>        | DB Site replication from a master DB has failed.                    |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | Remote Node Name + HA resource name (if Policy 0, no resource name) |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 300   |
| <b>OID</b>                | 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 \(MOS\)](#).

**31136 - DB Site Replication Precedence Relaxed**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | REPL  |
| <b>Description</b>      | Standby Site Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Site Databases to update as fast as possible. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | Remote Node Name + HA resource name (if Policy 0, no resource name)   |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 150   |
| <b>OID</b>              | comcolDbSiteRepPrecRelaxedNotify  |
| <b>Recovery</b>         | No action required.   |

**31137 - DB Site Replication Latency Over Threshold**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | REPL  |
| <b>Description</b>        | DB Site Replication latency has exceeded thresholds.                |
| <b>Severity</b>           | Major   |
| <b>Instance</b>           | Remote Node Name + HA resource name (if Policy 0, no resource name) |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 300   |
| <b>OID</b>                | 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 \(MOS\)](#).

**31140 - Database perl fault**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | SW  |
| <b>Description:</b> | Perl interface to Database is impaired by a s/w fault                                   |
| <b>Severity:</b>    | Minor   |
| <b>Instance:</b>    | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |

|                            |                         |
|----------------------------|-------------------------|
| <b>HA Score:</b>           | Normal                  |
| <b>Auto Clear Seconds:</b> | 300                     |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31145 - Database SQL fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | SQL interface to Database is impaired by a s/w fault                                    |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31146 - DB mastership fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | DB replication is impaired due to no mastering process (inetrep/inetrep).               |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolDbMastershipFaultNotify   |

**Recovery:**

1. Export event history for the given server.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

**31147 - DB upsynclog overrun**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | UpSyncLog is not big enough for (WAN) replication.                                      |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31148 - DB lock error detected**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DB   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31149 - DB Late Write Nonactive**

|                    |   |
|--------------------|---|
| <b>Alarm Group</b> | DB  |
| <b>Description</b> | Application wrote to database while HA role change from active was in progress. |

|                           |                         |
|---------------------------|-------------------------|
| <b>Severity</b>           | Minor                   |
| <b>Instance</b>           | HA resource name        |
| <b>HA Score</b>           | Normal                  |
| <b>Auto Clear Seconds</b> | 3600                    |
| <b>OID</b>                | comcolDbLateWriteNotify |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**31200 - Process management fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The process manager (procmgr) is impaired by a s/w fault                                |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31201 - Process not running**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PROC  |
| <b>Description:</b>        | A managed process cannot be started or has unexpectedly terminated                      |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolProcNotRunningNotify  |

**Recovery:**

1. This alarm indicates that the managed process exited unexpectedly due to a memory fault, but the process was automatically restarted.
2. It is recommended to collect savelogs and contact [My Oracle Support \(MOS\)](#).

**31202 - Unkillable zombie process**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PROC  |
| <b>Description:</b>        | A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr               |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31206 - Process mgmt monitoring fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The process manager monitor (pm.watchdog) is impaired by a s/w fault                    |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31207 - Process resource monitoring fault**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | SW  |
| <b>Description:</b> | The process resource monitor (ProcWatch) is impaired by a s/w fault |
| <b>Severity:</b>    | Minor   |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31208 - IP port server fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The run environment port mapper (re.portmap) is impaired by a s/w fault                 |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31209 - Hostname lookup failed**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | Unable to resolve a hostname specified in the NodeInfo table                            |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31213 - Process scheduler fault

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The process scheduler (ProcSched/runat) is impaired by a s/w fault                      |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31214 - Scheduled process fault

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PROC  |
| <b>Description:</b>        | A scheduled process cannot be executed or abnormally terminated                         |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31215 - Process resources exceeded

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | SW   |
| <b>Description:</b> | A process is consuming excessive system resources. |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 14400   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31216 - SysMetric configuration error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | A SysMetric Configuration table contains invalid data                                   |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolSysMetricConfigErrorNotify  |

**Recovery:**

1. This alarm indicates a system metric is configured incorrectly.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

**31217 - Network Health Warning**

|                           |                                  |
|---------------------------|----------------------------------|
| <b>Alarm Group</b>        | SW                               |
| <b>Description</b>        | Missed Heartbeats Detected       |
| <b>Severity</b>           | Minor                            |
| <b>Instance</b>           | IP Address                       |
| <b>HA Score</b>           | Normal                           |
| <b>Auto Clear Seconds</b> | 300                              |
| <b>OID</b>                | 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 \(MOS\)](#).

**31220 - HA configuration monitor fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The HA configuration monitor is impaired by a s/w fault.                                |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaCfgMonitorFaultNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**31221 - HA alarm monitor fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The high availability alarm monitor is impaired by a s/w fault                          |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaAlarmMonitorFaultNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**31222 - HA not configured**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | High availability is disabled due to system configuration                               |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaNotConfiguredNotify   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 31223 - HA Heartbeat transmit failure

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | The high availability monitor failed to send heartbeat.                                 |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31224 - HA configuration error

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | High availability configuration error   |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31225 - HA service start failure

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | HA   |
| <b>Description:</b> | The required high availability resource failed to start. |
| <b>Severity:</b>    | Major  |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | comcolHaSvcStartFailureNotify   |

**Recovery:**

1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, it is recommended to contact [My Oracle Support \(MOS\)](#).

**31226 - HA availability status degraded**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | The high availability status is degraded due to raised alarms.                          |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31227 - HA availability status failed**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | The high availability status is failed due to raised alarms.                            |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | N/A   |
| <b>OID:</b>                | 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, contact [My Oracle Support \(MOS\)](#).

### 31228 - HA standby offline

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | High availability standby server is offline.  |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | comcolHaStandbyOfflineNotify  |

#### Recovery:

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

### 31229 - HA score changed

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | High availability health score changed  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaScoreChangeNotify   |

#### Recovery:

Status message - no action required.

### 31230 - Recent alarm processing fault

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | SW   |
| <b>Description:</b> | The recent alarm event manager (raclerk) is impaired by a s/w fault. |
| <b>Severity:</b>    | Minor  |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31231 - Platform alarm agent fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The platform alarm agent impaired by a s/w fault  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31232 - Late heartbeat warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | High availability server has not received a message on specified path within the configured interval. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr               |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaLateHeartbeatWarningNotify  |

**Recovery:**

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

### 31233 - HA Path Down

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | High availability path loss of connectivity   |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31234 - Untrusted Time Upon Initialization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | REPL   |
| <b>Description:</b>        | Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | comcolUtrustedTimeOnInitNotify   |

**Recovery:**

1. Correct NTP configuration.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**31235 - Untrusted Time After Initialization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | REPL   |
| <b>Description:</b>        | After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, etc. There are often accompanying Platform alarms to guide correction. Generally, applications remain running, but time-stamped data is likely incorrect, reports may be negatively affected, some behavior may be improper, etc. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | comcolUtrustedTimePostInitNotify   |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. Correct NTP configuration.</li> <li>2. If the problem persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a>.</li> </ol>   |

**31236 - HA Link Down**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | HA   |
| <b>Description:</b>        | High availability TCP link is down.  |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | Remote node being connected to plus the path identifier  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | comcolHaLinkDownNotify   |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>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.</li> <li>2. If communication fails at any other time, it is recommended to look for network connectivity issues on the primary network and/or contact <a href="#">My Oracle Support (MOS)</a>.</li> </ol> |

**31240 - Measurements collection fault**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | SW   |
| <b>Description:</b> | The measurements collector (statclerk) is impaired by a s/w fault. |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31250 - RE port mapping fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The IP service port mapper (re.portmap) is impaired by a s/w fault                      |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolRePortMappingFaultNotify  |

**Recovery:**

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

**31260 - SNMP Agent**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | The SNMP agent (cmsnmpa) is impaired by a s/w fault.                                    |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

### 31261 - SNMP Configuration Error

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | SW  |
| <b>Description</b>        | A SNMP configuration error was detected   |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | comcolAlarmSrcNode, comcolAlarmNumber, comcolAlarmInstance, comcolAlarmSeverity, comcolAlarmText, comcolAlarmInfo, comcolAlarmGroup, comcolServerHostname, comcolAlarmSequence, comcolAlarmTimestamp, comcolAlarmEventType, comcolAlarmProbableCause, comcolAlarmAdditionalInfo |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | comcolSnmpConfigNotify  |

#### Recovery

1. Export event history for the given server and all processes.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 31270 - Logging output

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | SW  |
| <b>Description:</b>        | Logging output set to Above Normal  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolLoggingOutputNotify   |

#### Recovery:

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

### 31280 - HA Active to Standby transition

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | HA                                       |
| <b>Description:</b> | HA active to standby activity transition |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31281 - HA Standby to Active transition**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA standby to active activity transition  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31282 - HA Management Fault**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | The HA manager (cmha) is impaired by a software fault.                                  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31283 - Lost Communication with server**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | Highly available server failed to receive mate heartbeats                               |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

**31284 - HA Remote Subscriber Heartbeat Warning**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | HA   |
| <b>Description:</b>        | High availability remote subscriber has not received a heartbeat within the configured interval. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr          |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | 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 \(MOS\)](#).

**31285 - HA Node Join Recovery Entry**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | HA   |
| <b>Description:</b> | High availability node join recovery entered |
| <b>Severity:</b>    | Info   |

|                            |  |
|----------------------------|--|
| <b>Instance:</b>           | Cluster set key of the DC outputting the event |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | comcolHaSbrEntryNotify                         |

**Recovery:**

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

**31286 - HA Node Join Recovery Plan**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | HA   |
| <b>Description:</b>        | High availability node join recovery plan                    |
| <b>Severity:</b>           | Info   |
| <b>Instance:</b>           | Names of HA Policies (as defined in HA policy configuration) |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | comcolHaSbrPlanNotify  |

**Recovery:**

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

**31287 - HA Node Join Recovery Complete**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | HA   |
| <b>Description:</b>        | High availability node join recovery complete                |
| <b>Severity:</b>           | Info   |
| <b>Instance:</b>           | Names of HA Policies (as defined in HA policy configuration) |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 300  |
| <b>OID:</b>                | comcolHaSbrCompleteNotify                                    |

**Recovery:**

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

**31288 - HA Site Configuration Error**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | HA   |
| <b>Description</b>        | High availability site configuration error |
| <b>Severity</b>           | Critical                                   |
| <b>Instance</b>           | GroupName, Policy ID, Site Name            |
| <b>HA Score</b>           | Normal                                     |
| <b>Auto Clear Seconds</b> | 0 (zero)                                   |
| <b>OID</b>                | comcolHaBadSiteCfgNotify                   |

**Recovery**

If this alarm does not clear after correcting the configuration, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**31290 - HA Process Status**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA manager (cmha) status  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaProcessStatusNotify   |

**Recovery:**

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

**31291 - HA Election Status**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA DC Election status   |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaElectionStatusNotify  |

**Recovery:**

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

### 31292 - HA Policy Status

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA Policy plan status   |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaPolicyStatusNotify  |

**Recovery:**

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

### 31293 - HA Resource Link Status

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA ResourceAgent Link status  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaRaLinkStatusNotify  |

**Recovery:**

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

### 31294 - HA Resource Status

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA Resource registration status   |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaResourceStatusNotify  |

**Recovery:**

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

**31295 - HA Action Status**

|                            |                            |
|----------------------------|----------------------------|
| <b>Alarm Group:</b>        | HA                         |
| <b>Description:</b>        | HA Resource action status  |
| <b>Severity:</b>           | Info                       |
| <b>Instance</b>            | N/A                        |
| <b>HA Score:</b>           | Normal                     |
| <b>Auto Clear Seconds:</b> | 300                        |
| <b>OID:</b>                | comcolHaActionStatusNotify |

**Recovery:**

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

**31296 - HA Monitor Status**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA Monitor action status  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaMonitorStatusNotify   |

**Recovery:**

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

**31297 - HA Resource Agent Info**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA Resource Agent Info  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaRaInfoNotify  |

**Recovery:**

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

**31298 - HA Resource Agent Detail**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | Resource Agent application detailed information   |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaRaDetailNotify  |

**Recovery:**

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

**31299 - HA Notification Status**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA Notification status  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |
| <b>OID:</b>                | comcolHaNotificationNotify  |

**Recovery:**

No action required.

**31300 - HA Control Status**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | HA  |
| <b>Description:</b>        | HA Control action status  |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300   |

**OID:** comcolHaControlNotify

**Recovery:**  
No action required.

### 31301 - HA Topology Events

**Alarm Group:** HA  
**Description:** HA Topology events  
**Severity:** Info  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDsrHaTopologyNotify  
**Recovery:**  
No action required.

### 31322 - HA Configuration Error

**Alarm Group** HA  
**Description** High availability configuration error  
**Severity** Minor  
**Instance** NodeID, or HA Tunnel ID  
**HA Score** Normal  
**Auto Clear Seconds** 0 (zero)  
**OID** comcolHaBadCfgNotify

**Recovery**  
It is recommended to contact [My Oracle Support \(MOS\)](#).

### 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32106 - Power Supply 3 Failure**

**Alarm Group:** PLAT  
**Description:** Power Supply 3 Failure  
**Severity:** Critical

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdPowerSupply3Failure  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32107 - Raid Feed Unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | Raid Feed Unavailable   |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdRaidFeedUnavailable  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32108 - Raid Power 1 Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | Raid Power 1 Failure  |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdRaidPower1Failure  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32109 - Raid Power 2 Failure**

|                     |                      |
|---------------------|----------------------|
| <b>Alarm Group:</b> | PLAT                 |
| <b>Description:</b> | Raid Power 2 Failure |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdRaidPower2Failure  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32110 - Raid Power 3 Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | Raid Power 3 Failure  |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdRaidPower3Failure  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32111 - Device Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | Device Failure  |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDeviceFailure  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32112 - Device Interface Failure**

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | PLAT |
|---------------------|------|

|                            |   |
|----------------------------|---|
| <b>Description:</b>        | Device Interface Failure  |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDeviceIfFailure  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32113 - Uncorrectable ECC memory error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdEccUncorrectableError   |
| <b>Alarm ID:</b>           | TKSPLATCR14  |

**Recovery:**

Contact the hardware vendor to request hardware replacement.

**32114 - SNMP get failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | The server failed to receive SNMP information from the switch.                          |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdSNMPGetFailure   |
| <b>Alarm ID:</b>           | TKSPLATCR15   |

**Recovery:**

1. Verify device is active and responds to the ping command.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**32115 - TPD NTP Daemon Not Synchronized Failure**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                                      |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdNTPDaemonNotSynchronizedFailure   |
| <b>Alarm ID:</b>           | TKSPLATCR16  |

**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) 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 \(MOS\)](#).

**32116 - TPD Server's Time Has Gone Backwards**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good. |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdNTPTimeGoneBackwards   |
| <b>Alarm ID:</b>           | TKSPLATCR17   |

**Recovery:**

1. Verify NTP settings and that NTP sources are providing accurate time.
  - 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 the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**32117 - TPD NTP Offset Check Failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                                     |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | ntpOffsetCheckFailure   |
| <b>Alarm ID:</b>           | TKSPLATCR18   |

**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 \(MOS\)](#).

### 32300 - Server fan failure

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdFanError  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

### 32301 - Server internal disk error

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 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 \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 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 \(MOS\)](#) 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 \(MOS\)](#) 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 \(MOS\)](#) 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**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 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 \(MOS\)](#) and provide the system health check output and process swap usage.

### 32308 - Server provisioning network error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdProvNetworkError  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

### 32309 - Eagle Network A Error

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | Critical   |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdEagleNetworkAError   |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32310 - Eagle Network B Error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdEagleNetworkBError  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32311 - Sync Network Error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdSyncNetworkError  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

**32312 - Server disk space shortage error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that one of the following conditions has occurred: <ul style="list-style-type: none"> <li>• 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.</li> <li>• More than 90% of the total number of available files have been allocated on the file system.</li> <li>• A file system has a different number of blocks than it had when installed.</li> </ul> |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDiskSpaceShortageError  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the system health check output and provide additional file system output.

**32313 - Server default route network error**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | 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.

|                  |       |
|------------------|-------|
| <b>Severity:</b> | Major |
|------------------|-------|

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#).
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 \(MOS\)](#).
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 \(MOS\)](#).

**32314 - Server temperature error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | The internal temperature within the server is unacceptably high.                        |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdServerTemperatureError   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

### 32315 - Server mainboard voltage error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdServerMainboardVoltageError   |
| <b>Alarm ID:</b>           | TKSPLATMA16  |

**Recovery:**

1. Run syscheck in verbose mode.
2. If the alarm persists, it is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

### 32316 - Server power feed error

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | 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. |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdPowerFeedError   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

**32317 - Server disk health test error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | Either the hard drive has failed or failure is imminent.                                |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDiskHealthError  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the system health check output. .

### 32318 - Server disk unavailable error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDiskUnavailableError  |
| <b>Alarm ID:</b>           | TKSPLATMA19  |

#### Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

### 32319 - Device error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the offboard storage server had a problem with its disk volume filling up. |
| <b>Severity:</b>           | Major  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDeviceError   |
| <b>Alarm ID:</b>           | TKSPLATMA20  |

#### Recovery

It is recommended to contact the [My Oracle Support \(MOS\)](#).

**32320 - Device interface error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that the IP bond is either not configured or down.                 |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDeviceIfError  |
| <b>Alarm ID:</b>           | TKSPLATMA21   |

**Recovery:**

1. Run syscheck in verbose mode.
2. Investigate the failed bond, and slave devices, configuration:
  1. 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:
  1. cat /proc/net/bonding/bondX, where X is bond designation
  2. ethtool <slave device>
4. If bond, and slaves, are healthy attempt to administratively bring bond up:
  1. ifup bondX
5. If the problem has not been resolved, it is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output and the output of the above investigation.

**32321 - Correctable ECC memory error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdEccCorrectableError   |
| <b>Alarm ID:</b>           | 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**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that power supply 1 (feed A) has failed.                           |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdPowerSupply1Error  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the syscheck verbose output. Power supply 1 (feed A) will probably need to be replaced.

**32323 - Power Supply B error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that power supply 2 (feed B) has failed.                           |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdPowerSupply2Error  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the syscheck verbose output. Power supply 2 (feed B) will probably need to be replaced.

### 32324 - Breaker panel feed error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the server is not receiving information from the breaker panel relays. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr          |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdBrkPnlFeedError   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) to request that the breaker panel be replaced.

### 32325 - Breaker panel breaker error

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | <p>This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see <a href="#">Figure 16: Breaker Panel LEDs</a>) identify whether the fault occurred on the input power or the output power, as follows:</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p><b>Note:</b> 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.</p> |

- 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.

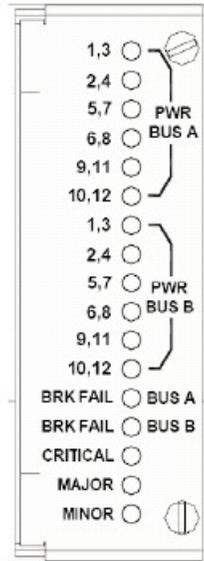


Figure 16: Breaker Panel LEDs

**Severity:** Major

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

**HA Score:** Normal

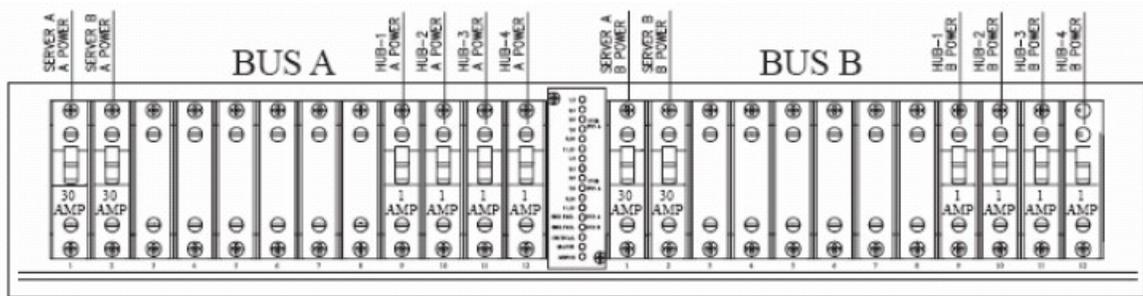
**Auto Clear Seconds:** 0 (zero)

**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 17: 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.
  1. If the LEDs are now illuminated Green, the issue has been resolved. Proceed to step 4 to verify that the alarm has been cleared.
  2. 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
  1. 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.
  2. 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 \(MOS\)](#)

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 run syscheck and contact [My Oracle Support \(MOS\)](#)
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 \(MOS\)](#)

### 32326 - Breaker panel monitoring error

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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.<br><br><b>Note:</b> 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: <ul style="list-style-type: none"> <li>• 32324 – Breaker panel feed error</li> <li>• 32325 – Breaker panel breaker error</li> </ul> until the Breaker Panel Monitoring Error has been corrected. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdBrkPnlMntError   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#)

**32327 - Server HA Keepalive error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdHaKeepaliveError  |
| <b>Alarm ID:</b>           | TKSPLATMA28  |

**Recovery:**

1. Determine if the mate server is currently down and bring it up if possible.
2. Determine if the keepalive interface is down.
3. Determine if heartbeat is running (service TKLCha status).

**Note:** This step may require command line ability.

4. It is recommended to contact [My Oracle Support \(MOS\)](#).

**32328 - DRBD is unavailable**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDrbdUnavailable  |
| <b>Alarm ID:</b>           | TKSPLATMA29   |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32329 - DRBD is not replicating**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDrbdNotReplicating  |
| <b>Alarm ID:</b>           | TKSPLATMA30  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32330 - DRBD peer problem**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDrbdPeerProblem   |
| <b>Alarm ID:</b>           | TKSPLATMA31  |

**Recovery**

It is recommended to contact the [My Oracle Support \(MOS\)](#).

**32331 - HP disk problem**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | 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. |

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHpDiskProblem  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the system health check output. The disk may need to be replaced.

**32332 - HP Smart Array controller problem**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHpDiskCtrlrProblem   |
| <b>Alarm ID:</b>           | TKSPLATMA33   |

**Recovery:**

1. Run syscheck in verbose mode.
2. If condition persists, it is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

**32333 - HP hpacucliStatus utility problem**

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | PLAT |
|---------------------|------|

|                            |   |
|----------------------------|---|
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHPACUCLIProblem  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the system health check output, and savelogs\_plat output.

**32334 - Multipath device access link problem**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                                  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdMpathDeviceProblem  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32335 - Switch link down error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | The link is down.   |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdSwitchLinkDownError  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) to determine who should verify port settings on both the server and the switch.

**32336 - Half Open Socket Limit**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHalfOpenSockLimit  |
| <b>Alarm ID:</b>           | 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.

- It is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output and collected data.

### 32337 - Flash Program Failure

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that there was an error while trying to update the firmware flash on the E5-APP-B cards. |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                       |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdFlashProgramFailure  |
| <b>Alarm ID:</b>           | TKSPLATMA38   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 32338 - Serial Mezzanine Unseated

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that a connection to the serial mezzanine board may not be properly seated. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr          |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdSerialMezzUnseated  |
| <b>Alarm ID:</b>           | TKSPLATMA39  |

**Recovery:**

- Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.
- It is recommended to contact [My Oracle Support \(MOS\)](#) if reseating the cables does not clear the alarm.

### 32339 - TPD Max Number Of Running Processes Error

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | PLAT |
|---------------------|------|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | This alarm indicates that the maximum number of running processes has reached the major threshold. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr            |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdMaxPidLimit   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the system health check output, and pid output.

**32340 - TPD NTP Daemon Not Synchronized Error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdNTPDaemonNotSynchronizedError   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

### 32341 - TPD NTP Daemon Not Synchronized Error

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdNTPDaemonNeverSynchronized  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

**32342 - NTP Offset Check Error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                                  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | ntpOffsetCheckError  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

**32343 - TPD RAID disk**

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | This alarms indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck. |
| <b>Severity:</b>    | Major  |
| <b>Instance:</b>    | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |

|                            |                |
|----------------------------|----------------|
| <b>HA Score:</b>           | Normal         |
| <b>Auto Clear Seconds:</b> | 0 (zero)       |
| <b>OID:</b>                | tpdDiskProblem |
| <b>Alarm ID:</b>           | TKSPLATMA44    |

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

**32344 - TPD RAID controller problem**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarms indicates that RAID controller needs intervention.                          |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDiskCtrlrProblem   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the system health check output.

**32345 - Server Upgrade snapshot(s) invalid**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible. |
| <b>Severity:</b>           | Major  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr      |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdUpgradeSnapshotInvalid  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

**32346 - OEM hardware management service reports an error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarms indicates that OEM hardware management service reports an error.            |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdOEMHardware  |
| <b>Alarm ID:</b>           | TKSPLATMA47   |

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

**32347 - The hwmgmtcliStatus daemon needs intervention**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarms indicates the hwmgmtcliStatus daemon is not running or is not responding.   |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHWMGMTCLIProblem   |
| <b>Alarm ID:</b>           | TKSPLATMA47   |

**Recovery:**

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the hwmgmt process is running. If not running verify that it was not administratively stopped.

- Executing "service hwmgmt status" should produce output indicating that the process is running.
  - If not running attempt to start process "service hwmgmt status".
4. Determine if the TKLChwmgmtcli process is running. If not running verify that it was not administratively stopped.
    - 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 hwmgmt process is hung, proceed with next step.
  6. It is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

### 32348 - FIPS subsystem problem

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates the FIPS subsystem is not running or has encountered errors.       |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdFipsSubsystemProblem   |

#### Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

### 32349 - File Tampering

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates HIDS has detected file tampering.                                  |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHidsFileTampering  |

#### Recovery:

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32350 - Security Process Terminated**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that the security process monitor is not running.                  |
| <b>Severity:</b>           | Major   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdSecurityProcessDown  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32500 - Server disk space shortage warning**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that one of the following conditions has occurred: <ul style="list-style-type: none"> <li>• 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.</li> <li>• More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.</li> </ul> |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDiskSpaceShortageWarning  |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#), provide the system health check output, and provide additional file system output.

**32501 - Server application process error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdApplicationProcessError   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#) and provide the syscheck output.

**32502 - Server hardware configuration error**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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). |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHardwareConfigError  |
| <b>Alarm ID:</b>           | TKSPLATMI3  |

**Recovery:**

1. Run syscheck in verbose mode.
2. Contact the hardware vendor to request a hardware replacement.

**32503 - Server RAM shortage warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr               |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdRamShortageWarning   |
| <b>Alarm ID:</b>           | TKSPLATMI4  |

**Recovery**

1. Refer to MPS-specific documentation for information regarding this alarm.
2. It is recommended to contact the [My Oracle Support \(MOS\)](#).

**32504 - Software Configuration Error**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm is generated by the MPS syscheck software package and is not part of the PLAT distribution. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdSoftwareConfigError   |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32505 - Server swap space shortage warning**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | 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. |
|                     | <b>Note:</b> 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.

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdSwapSpaceShortageWarning   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#), provide the system health check output, and process swap usage.

**32506 - Server default router not defined**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | 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.

|                            |   |
|----------------------------|---|
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDefaultRouteNotDefined   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

### 32507 - Server temperature warning

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdServerTemperatureWarning   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

**32508 - Server core file detected**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that an application process has failed and debug information is available. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr         |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdServerCoreFileDetected   |
| <b>Alarm ID:</b>           | TKSPLATMI9  |

**Recovery:**

1. It is recommended to contact [My Oracle Support \(MOS\)](#) 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 \(MOS\)](#) 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**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdNTPDaemonNotSynchronizedWarning  |
| <b>Alarm ID:</b>           | 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:** 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 \(MOS\)](#).

### 32510 - CMOS battery voltage low

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdCMOSBatteryVoltageLow  |
| <b>Alarm ID:</b>           | TKSPLATMI11   |
| <b>Recovery:</b>           | It is recommended to contact <a href="#">My Oracle Support (MOS)</a> .  |

### 32511 - Server disk self test warning

|                     |  |
|---------------------|--|
| <b>Alarm Group:</b> | PLAT   |
| <b>Description:</b> | A non-fatal disk issue (such as a sector cannot be read) exists. |
| <b>Severity:</b>    | Minor  |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdSmartTestWarn  |
| <b>Alarm ID:</b>           | TKSPLATMI12   |

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

**32512 - Device warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that either we are unable to perform an <code>snmpget</code> command on the configured SNMP OID or the value returned failed the specified comparison operation. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDeviceWarn   |
| <b>Alarm ID:</b>           | TKSPLATMI13   |

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

**32513 - Device interface warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm can be generated by either an SNMP trap or an IP bond error.                 |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDeviceIfWarn   |

**Alarm ID:** TKSPLATMI14

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

### 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

### 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32516 - Server HA Active to Standby transition**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the server is in the process of transitioning HA state from Active to Standby. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdHaActiveToStandbyTrans  |
| <b>Alarm ID:</b>           | TKSPLATMI17  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32517 - Server HA Standby to Active transition**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the server is in the process of transitioning HA state from Standby to Active. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdHaStandbyToActiveTrans  |
| <b>Alarm ID:</b>           | TKSPLATMI18  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32518 - Platform Health Check failure**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | This alarm is used to indicate a configuration error.                                   |
| <b>Severity:</b>    | Minor   |
| <b>Instance:</b>    | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>    | Normal  |

**Auto Clear Seconds:** 0 (zero)  
**OID:** tpdHealthCheckFailed  
**Alarm ID:** TKSPLATMI19

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**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:** 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 \(MOS\)](#).

**32520 - NTP Stratum Check failure**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | ntpStratumCheckFailed   |
| <b>Alarm ID:</b>           | 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:** 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 \(MOS\)](#).

**32521 - SAS Presence Sensor Missing**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | This alarm indicates that the T1200 server drive sensor is not working. |
| <b>Severity:</b>    | Minor   |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | sasPresenceSensorMissing  |
| <b>Alarm ID:</b>           | TKSPLATMI22   |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) to get a replacement sensor.

**32522 - SAS Drive Missing**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the number of drives configured for this server is not being detected. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr          |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | sasDriveMissing  |
| <b>Alarm ID:</b>           | TKSPLATMI23  |

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32523 - DRBD failover busy**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdDrbdFailoverBusy  |
| <b>Alarm ID:</b>           | TKSPLATMI24  |

**Recovery**

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 \(MOS\)](#).

### 32524 - HP disk resync

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdHpDiskResync  |
| <b>Alarm ID:</b>           | TKSPLATMI25  |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. Run syscheck in verbose mode.</li> <li>2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck.</li> <li>3. If the alarm persists, it is recommended to contact <a href="#">My Oracle Support (MOS)</a> and provide the syscheck output.</li> </ol>  |

### 32525 - Telco Fan Warning

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that the Telco switch has detected an issue with an internal fan.  |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdTelcoFanWarning  |
| <b>Alarm ID:</b>           | TKSPLATMI26   |

**Recovery:**

Contact the vendor to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.

**Note:** *My Oracle Support (MOS)* personnel can perform an `snmpget` command or log into the switch to get detailed fan status information.

**32526 - Telco Temperature Warning**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                      |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdTelcoTemperatureWarning   |
| <b>Alarm ID:</b>           | 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 (MOS)*.

**32527 - Telco Power Supply Warning**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                      |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdTelcoPowerSupplyWarning   |
| <b>Alarm ID:</b>           | 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 (MOS)* 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**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdInvalidBiosValue   |
| <b>Alarm ID:</b>           | TKSPLATMI29   |

**Recovery:**

Change the BIOS values to the expected values which involves re-booting the server. It is recommended to contact [My Oracle Support \(MOS\)](#) for directions on changing the BIOS.

**32529 - Server Kernel Dump File Detected**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that the kernel has crashed and debug information is available.    |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdServerKernelDumpFileDetected   |
| <b>Alarm ID:</b>           | TKSPLATMI30   |

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

**32530 - TPD Upgrade Failed**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | This alarm indicates that a TPD upgrade has failed. |
| <b>Severity:</b>    | Minor   |

|                            |   |
|----------------------------|---|
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | TpdServerUpgradeFailed  |
| <b>Alarm ID:</b>           | TKSPLATMI31   |
| <b>Recovery:</b>           | It is recommended to contact <a href="#">My Oracle Support (MOS)</a> .                  |

### 32531 - Half Open Socket Warning Limit

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdHalfOpenSocketWarning  |
| <b>Alarm ID:</b>           | TKSPLATMI32   |
| <b>Recovery:</b>           | <ol style="list-style-type: none"> <li>1. Run syscheck in verbose mode.</li> <li>2. It is recommended to contact <a href="#">My Oracle Support (MOS)</a>.</li> </ol>                  |

### 32532 - Server Upgrade Pending Accept/Reject

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that an upgrade occurred but has not been accepted or rejected yet. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdServerUpgradePendingAccept  |
| <b>Alarm ID:</b>           | TKSPLATMI33  |

**Recovery:**

Follow the steps in the application procedure to accept or reject the upgrade.

**32533 - TPD Max Number Of Running Processes Warning**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | This alarm indicates that the maximum number of running processes has reached the minor threshold. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr            |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdMaxPidWarning   |
| <b>Alarm ID:</b>           | TKSPLATMI34  |

**Recovery:**

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

**32534 - TPD NTP Source Is Bad Warning**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source. |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr                                   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdNTPSourceIsBad   |
| <b>Alarm ID:</b>           | 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:** 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 \(MOS\)](#).

### 32535 - TPD RAID disk resync

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | PLAT  |
| <b>Description:</b>        | 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). |
| <b>Severity:</b>           | Minor   |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | tpdDiskResync   |
| <b>Alarm ID:</b>           | 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 \(MOS\)](#).

### 32536 - TPD Server Upgrade snapshot(s) warning

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | PLAT  |
| <b>Description:</b> | 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. |
| <b>Severity:</b>    | Minor   |
| <b>Instance:</b>    | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr   |

|                            |                           |
|----------------------------|---------------------------|
| <b>HA Score:</b>           | Normal                    |
| <b>Auto Clear Seconds:</b> | 0 (zero)                  |
| <b>OID:</b>                | tpdUpgradeSnapshotWarning |
| <b>Alarm ID:</b>           | TKSPLATMI37               |

**Recovery:**

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. It is recommended to contact [My Oracle Support \(MOS\)](#)

**32537 - FIPS subsystem warning event**

|                            |  |
|----------------------------|--|
| <b>Alarm Type:</b>         | PLAT   |
| <b>Description:</b>        | This alarm indicates that the FIPS subsystem requires a reboot in order to complete configuration. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr            |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdFipsSubsystemWarning  |

**Recovery**

If alarm doesn't clear on its own, it is recommended to contact [My Oracle Support \(MOS\)](#).

**32538 - Platform Data Collection Error**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | PLAT  |
| <b>Description</b>        | Platform Data Collection Error  |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | 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 \(MOS\)](#).

**32539 - Server Patch Pending Accept/Reject**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | PLAT  |
| <b>Description</b>        | Server Patch Pending Accept/Reject  |
| <b>Severity</b>           | Minor   |
| <b>Instance</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | tpdServerPatchPendingAccept   |

**Recovery**

Accept or reject the patch per the application documentation procedure.

**32540 - CPU Power limit mismatch**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | PLAT   |
| <b>Description:</b>        | The BIOS setting for CPU Power Limit is different than expected. |
| <b>Severity:</b>           | Minor  |
| <b>Instance:</b>           | N/A  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | tpdCpuPowerLimitMismatch   |
| <b>Alarm ID:</b>           | TKSPLATMI41  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32700 - Telco Switch Notification**

|                           |   |
|---------------------------|---|
| <b>Alarm Group:</b>       | PLAT  |
| <b>Description</b>        | Telco Switch Notification   |
| <b>Severity</b>           | Info  |
| <b>Instance</b>           | May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 86400   |
| <b>OID</b>                | tpdTelcoSwitchNotification  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32701 - HIDS Initialized**

|                          |  |
|--------------------------|--|
| <b>Alarm Group:</b>      | PLAT                                       |
| <b>Description:</b>      | This alarm indicates HIDS was initialized. |
| <b>Default Severity:</b> | Info                                       |
| <b>OID:</b>              | tpdHidsBaselineCreated                     |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32702 - HIDS Baseline Deleted**

|                          |                            |
|--------------------------|----------------------------|
| <b>Alarm Group:</b>      | PLAT                       |
| <b>Description:</b>      | HIDS baseline was deleted. |
| <b>Default Severity:</b> | Info                       |
| <b>OID:</b>              | tpdHidsBaselineDeleted     |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32703 - HIDS Enabled**

|                          |                   |
|--------------------------|-------------------|
| <b>Alarm Group:</b>      | PLAT              |
| <b>Description:</b>      | HIDS was enabled. |
| <b>Default Severity:</b> | Info              |
| <b>OID:</b>              | tpdHidsEnabled    |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32704 - HIDS Disabled**

|                          |                    |
|--------------------------|--------------------|
| <b>Alarm Group:</b>      | PLAT               |
| <b>Description:</b>      | HIDS was disabled. |
| <b>Default Severity:</b> | Info               |
| <b>OID:</b>              | tpdHidsDisabled    |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32705 - HIDS Monitoring Suspended**

|                          |                            |
|--------------------------|----------------------------|
| <b>Alarm Group:</b>      | PLAT                       |
| <b>Description:</b>      | HIDS monitoring suspended. |
| <b>Default Severity:</b> | Info                       |
| <b>OID:</b>              | tpdHidsSuspended           |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32706 - HIDS Monitoring Resumed**

|                          |                          |
|--------------------------|--------------------------|
| <b>Alarm Group:</b>      | PLAT                     |
| <b>Description:</b>      | HIDS monitoring resumed. |
| <b>Default Severity:</b> | Info                     |
| <b>OID:</b>              | tpdHidsResumed           |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**32707 - HIDS Baseline Updated**

|                          |                        |
|--------------------------|------------------------|
| <b>Alarm Group:</b>      | PLAT                   |
| <b>Description:</b>      | HIDS baseline updated. |
| <b>Default Severity:</b> | Info                   |
| <b>OID:</b>              | tpdHidsBaselineUpdated |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#).

**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**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIWF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | None  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterDmiwfAppComagentProviderRegistrationFailureNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**33001 - Diameter-to-MAP Service Registration Failure on DA-MP**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIWF  |
| <b>Description:</b>        | DM-IWF application was unable to register for Diameter-to-MAP transaction service. Diameter-to-MAP transactions cannot be serviced by this DA-MP. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | None  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterDmiwfAppComagentUserRegistrationFailureNotify  |

**Recovery:**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**33002 - DM-IWF DA-MP not associated with a Place**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIWF  |
| <b>Description:</b>        | DM-IWF DA-MP server is not associated with an AppWorks Place. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | None  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for further assistance.

**33003 - Insufficient memory for DM-IWF**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIWF  |
| <b>Description:</b>        | DA-MP does not have sufficient memory to support DM-IWF |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | None  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterDmiwfAppInsufficientMemoryFailureNotify  |

**Recovery:**

1. If the VM:Database DA-MP profile is applied to the DA-MP (**Main Menu > 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 (**Main Menu > 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 (**Main Menu > 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 \(MOS\)](#) for further assistance on how to upgrade memory.

**33004 - DM-IWF Transaction Response Queue Utilization**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIWF  |
| <b>Description:</b>        | The DM-IWF Transaction Response Queue Utilization is approaching its maximum engineered capacity. |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | RxDmiwfTranRspMsgQueue, DM-IWF  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance.

### 33005 - DM-IWF PTR Pool Utilization

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | DIWF  |
| <b>Description:</b>        | 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. |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | RxDmiwfTranRspMsgQueue, DM-IWF  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 **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 **Main Menu > Diameter > Maintenance > Applications**. DM-IWF service provider status can be monitored from **Main Menu > Communication Agent > Maintenance > Routed Services Status**
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 33006 - MD-IWF Service Congestion

|                     |  |
|---------------------|--|
| <b>Event Group:</b> | DIWF   |
| <b>Description:</b> | DM-IWF could not forward a Request to MD-IWF due to MD-IWF Service Congestion. |
| <b>Severity:</b>    | Info   |
| <b>Instance:</b>    | <DAMPName>   |
| <b>HA Score:</b>    | 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 **Main Menu > Communication Agent > Maintenance > Routed Services Status**.
2. If the problem occurs frequently, it is recommended to contact [My Oracle Support \(MOS\)](#).

**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:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**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 allocate 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** 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 **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. 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 **Main Menu > Diameter > Maintenance > Applications**. DM-IWF service provider status can be monitored from **Main Menu > Communication Agent > Maintenance > Routed Services Status**
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 33009 - DM-IWF unexpected Answer response received from a SS7-MP

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | DIWF  |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <DAMPName>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 **Main Menu -> MAP-Diameter IWF -> Configuration -> MD-IWF Options** screen.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

### 33010 - MD-IWF ComAgent Connection exhausted

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | DIWF   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <DAMPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 **Main Menu -> MAP-Diameter IWF -> Configuration -> MD-IWF Options** screen.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**33011 - DM-IWF Answer Timeout**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | DIWF   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <DAMPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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: **Main Menu > MAP Interworking > Configuration > Options (MD-IWF tab)**.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**33012 - DM-IWF encode decode error**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | DIWF   |
| <b>Description:</b>      | The decoder has reported an error causing the Request to be discarded. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <DAMPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterDmiwfDecodeErrorNotify                                  |

**Recovery:**

If the problem persists, it is recommended contact [My Oracle Support \(MOS\)](#).

**33013 - DRL queue exhaustion**

|                     |      |
|---------------------|------|
| <b>Event Group:</b> | DIWF |
|---------------------|------|

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | DM-IWF failed to forward a Diameter message to DRL due to DRL queue exhaustion. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | <DAMPName>  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterDrlQueueExhaustionNotify   |

**Recovery:**

If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

**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**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | DIWF   |
| <b>Description:</b>        | DA-MP has been assigned a profile that is incompatible with DM-IWF |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | None   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterDmiwfAppIncompatibleProfileFailureNotify            |

**Recovery:**

1. If the DA-MP has been assigned a DA-MP profile (**Main Menu > Diameter > Configuration > DA-MPs > Profile Assignments**) other than those listed below, apply a compatible profile and restart DSR (**Main Menu > 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 Customer Care Center for assistance.
3. If needed, it is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**33015 - DM-IWF Diameter message size exceeded maximum supported size**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | DIWF   |
| <b>Description:</b>      | DM-IWF failed to forward the Diameter message to SS7-MP because the message size exceeds supported maximum message size. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | <DAMPName>   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterDmiwfMaxDiameterMsgSizeExceededNotify   |

**Recovery:**

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**

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | MIWF  |
| <b>Description:</b>        | The ingress message rate for the MD-IWF Application is approaching or exceeding its engineered traffic handling capacity. |
| <b>Severity:</b>           | Minor, Major, Critical  |
| <b>Instance:</b>           | RxMdIwfIngressMsgRate, MD-IWF   |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 **Main Menu > 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 **Main Menu > 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 (MOS)* for further assistance.

### 33051 - MD-IWF Application Degraded or Unavailable

|                            |   |
|----------------------------|---|
| <b>Alarm Group:</b>        | MIWF  |
| <b>Description:</b>        | MD-IWF Application operational status is Degraded or Unavailable. |
| <b>Severity:</b>           | Major, Critical   |
| <b>Instance:</b>           | None  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | eagleXgDiameterMdIwfAppIDegradedOrUnavailableNotify               |

#### 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 **Main Menu > 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 (MOS)*.

### 33052 - MD-IWF Notified that DM-IWF Service Status is Down

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | MIWF |
|---------------------|------|

|                            |   |
|----------------------------|---|
| <b>Description:</b>        | The MD-IWF is notified via ComAgent that the rolled-up DM-IWF Service Status is Down. |
| <b>Severity:</b>           | Critical  |
| <b>Instance:</b>           | None  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 0 (zero)  |
| <b>OID:</b>                | 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 \(MOS\)](#) for further assistance.

**33053 - MD-IWF DiamTrans Task Queue Utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | MIWF   |
| <b>Description:</b>        | The MD-IWF Application DiamTrans Task Queue Utilization is approaching its maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | RxMdIwfDiamTransMsgQueue (TaskID), MD-IWF  |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 **Main Menu > 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 **Main Menu > Alarms & Events**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**33054 - MD-IWF MapTrans Task Queue Utilization**

|                     |   |
|---------------------|---|
| <b>Alarm Group:</b> | MIWF  |
| <b>Description:</b> | The MD-IWF Application MapTrans Task Queue Utilization is approaching its maximum capacity. |
| <b>Severity:</b>    | Minor, Major, Critical  |
| <b>Instance:</b>    | RxMdIwfMapTransMsgQueue (TaskId), MD-IWF  |
| <b>HA Score:</b>    | 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 **Main Menu > 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 **Main Menu > Alarms & Events**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) 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 **Main Menu > 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 **Main Menu > Alarms & Events**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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:**

It is recommended to contact [My Oracle Support \(MOS\)](#) 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 **Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options**.
4. It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**33059 - MD-IWF MapToDiam PTR Utilization**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | MIWF   |
| <b>Description:</b>        | MD-IWF Application MapToDiam PTR Utilization is approaching its maximum engineered capacity. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | EvMdIwfMap2DiamPtrUtil, MD-IWF   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 **Main Menu > MAP Interworking > Configuration > MD-IWF Options**.
4. It is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**33060 - SS7-MP Profile Not Assigned**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | MIWF   |
| <b>Description:</b>        | An SS7-MP configuration profile has not been assigned to this SS7-MP |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | None   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | eagleXgDiameterSs7MpProfileNotAssignedNotify                         |

**Recovery**

1. If the SS7-MP has been assigned an MP Profile from an SO GUI **Main Menu > Diameter Common > MPs > Profile Assignment** other MD-IWF, apply a compatible profile and restart the mapiwf process from **Main Menu > Status & Manage > Server**.
2. If the SS7-MP has been assigned a compatible profile already, it is recommended to contact [My Oracle Support \(MOS\)](#) for further assistance.

**33062 - Insufficient Memory for MD-IWF**

|                     |      |
|---------------------|------|
| <b>Alarm Group:</b> | MIWF |
|---------------------|------|

|                            |  |
|----------------------------|--|
| <b>Description:</b>        | SS7-MP does not have sufficient memory to support MD-IWF |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | None   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for further assistance.

**33063 - MD-IWF SS7-MP not associated with a Place**

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | MIWF   |
| <b>Description:</b>        | The MD-IWF SS7-MP server is not associated with an AppWorks Place. |
| <b>Severity:</b>           | Critical   |
| <b>Instance:</b>           | None   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for further assistance.

**33065 - MD-IWF Resource Exhaustion**

|                            |   |
|----------------------------|---|
| <b>Event Group:</b>        | MIWF  |
| <b>Description:</b>        | MD-IWF Application is unable to process a message due to resource exhaustion. |
| <b>Severity:</b>           | Info  |
| <b>Instance:</b>           | mapiwf  |
| <b>HA Score:</b>           | Normal  |
| <b>Auto Clear Seconds:</b> | 300 seconds (5 minutes)   |
| <b>OID:</b>                | 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 \(MOS\)](#) for assistance if needed.

**33066 - MD-IWF orphan Diameter Answer message received**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | MIWF  |
| <b>Description:</b>      | MD-IWF Application received a Diameter Answer message for which no Pending Transaction record exists. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 **Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options NO GUI Screen**.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

**33067 - MD-IWF orphan MAP Response message received**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | MIWF   |
| <b>Description:</b>      | MD-IWF Application received a MAP response message for which no Pending Transaction record exists. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | mapiwf   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 **Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options**.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

**33068 - MD-IWF MAP Response timeout**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | MIWF  |
| <b>Description:</b>      | MD-IWF Application sent a MAP request message to the SS7 network, but timed out waiting for the MAP response. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 **Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

**33069 - MD-IWF Diameter Answer timeout**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | MIWF  |
| <b>Description:</b>      | MD-IWF Application sent a Diameter Request message to the DA-MP, but timed out waiting for the Diameter Answer. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 **Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

**33070 - MD-IWF Generated Diameter Answer error message due to Diameter Exception**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | MIWF   |
| <b>Description:</b>      | An error occurred while MD-IWF Application was processing a Diameter Request message, causing it generate a Diameter Answer error message. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | mapiwf   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterMdIwfGeneratedDiamErrorAnswerNotify   |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) if assistance is needed.

**33071 - MD-IWF Generated MAP Error Response due to MAP exception**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | MIWF   |
| <b>Description:</b>      | An error occurred while MD-IWF Application was processing a MAP request message, causing it generate a MAP response error message. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | mapiwf   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterMdIwfGeneratedMapErrorResponseNotify  |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) if assistance is needed.

**33072 - MD-IWF received TCAP Notice from SS7 network**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | MIWF  |
| <b>Description:</b>      | MD-IWF Application received a TCAP Notice from the SS7 network. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterMdIwfTcapNoticeRecdNotify                        |

**Recovery**

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**

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | MIWF  |
| <b>Description:</b>      | MD-IWF Application admin state was changed to Enabled on the SS7-MP |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | eagleXgDiameterMdIwfAdminStateEnabledNotify                         |

**Recovery**

No action required.

**33074 - MD-IWF admin state set to Disabled**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | MIWF   |
| <b>Description:</b>      | MD-IWF Application admin state was changed to Disabled on the SS7-MP |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | mapiwf   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | eagleXgDiameterMdIwfAdminStateDisabledNotify                         |

**Recovery**

No action required.

**33075 - MD-IWF received ComAgent error or DM-IWF NACK**

|                     |   |
|---------------------|---|
| <b>Event Group:</b> | MIWF  |
| <b>Description:</b> | MD-IWF sent a Diameter Request message to DM-IWF that resulted in a ComAgent error / timeout or in a DM-IWF NACK. |
| <b>Severity:</b>    | Info  |
| <b>Instance:</b>    | mapiwf  |
| <b>HA Score:</b>    | Normal  |

**Throttle Seconds:** 10  
**OID:** eagleXgDiameterMdIwfRcvdComAgtErrorOrDmiwfnckNotify

**Recovery**

No action required.

**33076 - MD-IWF received Diameter Answer 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**

This error is not expected to occur. It is recommended to contact [My Oracle Support \(MOS\)](#) 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 \(MOS\)](#) for assistance if needed.

### 33078 - MD-IWF received Diameter EIR message but Destination-Host AVP not present or not found in mapping table

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | MIWF   |
| <b>Description:</b>      | 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. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | mapiwf   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 10   |
| <b>OID:</b>              | 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 **Main Menu > MAP-Diameter IWF > Configuration > Diameter Identity GTA**.
3. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

### 33079 - MD-IWF message translation failed

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | MIWF  |
| <b>Description:</b>      | MD-IWF attempt to perform message translation was unsuccessful. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 \(MOS\)](#) for assistance if needed.

### 33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message

|                     |      |
|---------------------|------|
| <b>Event Group:</b> | MIWF |
|---------------------|------|

|                          |   |
|--------------------------|---|
| <b>Description:</b>      | EDL failure occurred while MD-IWF attempted to encode a Diameter message. |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | mapiwf  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 10  |
| <b>OID:</b>              | 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 \(MOS\)](#) 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**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | GLA  |
| <b>Description:</b>      | Message received was rejected because of a decoding failure. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | "MP"   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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 \(MOS\)](#).

### 33101 - GLA Incorrect Application ID or Command Code

|                          |   |
|--------------------------|---|
| <b>Event Group:</b>      | GLA   |
| <b>Description:</b>      | Message received was rejected because the Application ID was not GL (16777321) or the Command Code was not GGR (8388655). |
| <b>Severity:</b>         | Info  |
| <b>Instance:</b>         | "MP"  |
| <b>HA Score:</b>         | Normal  |
| <b>Throttle Seconds:</b> | 60  |
| <b>OID:</b>              | eagleXgDiameterGlaIncorrectAppIdOrCmdCodeNotify   |

**Recovery:**

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

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | GLA  |
| <b>Description:</b>      | Message received was rejected because it did not contain and IMSI or an MSISDN in a Subscription-ID AVP. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | "MP"   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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

|                     |     |
|---------------------|-----|
| <b>Event Group:</b> | GLA |
|---------------------|-----|

|                          |  |
|--------------------------|--|
| <b>Description:</b>      | GLA was unable to communicate with the pSBR-Binding due to a communications error. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | "MP"   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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 \(MOS\)](#).

**33104 - GLA Duplicate Subscriber ID**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | GLA  |
| <b>Description:</b>      | Message received was rejected because it contained both a User-Name AVP and a MSISDN AVP |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | "MP"   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 60   |
| <b>OID:</b>              | 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 the GQC and GQS to determine which node is inserting both AVPs and correct that node so that only one AVP is included in the GGR.

**33105 - Routing Attempt failed due to queue exhaustion**

|                          |  |
|--------------------------|--|
| <b>Event Group:</b>      | GLA  |
| <b>Description:</b>      | Message could not be routed because the internal "Answer Message Queue" to the DSR Relay Agent was full. |
| <b>Severity:</b>         | Info   |
| <b>Instance:</b>         | "MP"   |
| <b>HA Score:</b>         | Normal   |
| <b>Throttle Seconds:</b> | 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 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 \(MOS\)](#).

### 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 **Main Menu > 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 \(MOS\)](#) for assistance.

### 33121 - GLA pSBR-B Response Task Message Queue Utilization

|                            |  |
|----------------------------|--|
| <b>Alarm Group:</b>        | GLA  |
| <b>Description:</b>        | GLA's pSBR-B Response Message Queue Utilization is approaching its maximum capacity. |
| <b>Severity:</b>           | Minor, Major, Critical   |
| <b>Instance:</b>           | RxGlaResponseMsgQueue, GLA   |
| <b>HA Score:</b>           | Normal   |
| <b>Auto Clear Seconds:</b> | 0 (zero)   |
| <b>OID:</b>                | 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 \(MOS\)](#) 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

|                    |  |
|--------------------|--|
| <b>Event Type</b>  | DCA  |
| <b>Description</b> | Dsroam failed to create application version on DcaLifecycleSoam table. |

|                         |                                     |
|-------------------------|-------------------------------------|
| <b>Severity</b>         | Info                                |
| <b>Instance</b>         | DcaLifecycleNoam.verId              |
| <b>HA Score</b>         | Normal                              |
| <b>Throttle Seconds</b> | 60                                  |
| <b>OID</b>              | dcaDcaCreateAppVersionFailureNotify |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**33301 - Update Config Data Failure**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DCA  |
| <b>Description</b>      | Dsroam failed to synchronize configuration data on SO. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | ApplicationId.name                                     |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 60   |
| <b>OID</b>              | dcaDcaUpdateConfigDataFailureNotify                    |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**33302 - Delete Application Version Failure**

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DCA  |
| <b>Description</b>      | Dsroam failed to delete application version from DcaLifecycleSoam table. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | DcaLifecycleSoam.verId   |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 60   |
| <b>OID</b>              | dcaDcaDeleteAppVersionFailureNotify                                      |

**Recovery**

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**33303 - U-SBR Event Queue Utilization**

|                    |     |
|--------------------|-----|
| <b>Alarm Group</b> | DCA |
|--------------------|-----|

|                           |  |
|---------------------------|--|
| <b>Description</b>        | The DSR Application U-SBR Event Queue Utilization is approaching its maximum capacity. |
| <b>Severity</b>           | Minor, Major, Critical   |
| <b>Instance</b>           | RxDcaSbrEventMsgQueue [<DcaDalld.dalld>], DCA  |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | 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 **Main Menu > Alarms & Events**.

2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

**33304 - DCA Runtime Errors**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DCA  |
| <b>Description</b>        | The script generated runtime errors.   |
| <b>Severity</b>           | Critical   |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalld.shortName</i> ) prefixed with "DCA:" and thread pool (Request, Answer or SBR Event) |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 60   |
| <b>OID</b>                | dcaDSRAppRuntimeErrorNotify  |

**Recovery**

The error message generated by the Perl interpreter is included in the alarm's additional info.

Fix the error accordingly and recompile the Perl script, or replace the Trial/Production version (depending on whether the DA-MP is a Trial DA-MP or not) with another script version.

**Note:** Because the compilation occurs in parallel while the previously compiled script is still running (and hence keeps raising the alarm), a successful compilation will not immediately clear the alarm. There will be an auto clear latency of 20 seconds that will clear the alarm.

**33305 - DCA Procedure Not Found**

|                           |  |
|---------------------------|--|
| <b>Alarm Group</b>        | DCA  |
| <b>Description</b>        | The Perl interpreter attempts to invoke a non-existent procedure.  |
| <b>Severity</b>           | Critical   |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalld.shortName</i> ) prefixed with "DCA:" and thread pool (Request, Answer or SBR Event) |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 60   |
| <b>OID</b>                | dcaDSRAppProcedureNotFoundNotify   |

**Recovery**

The name of the missing procedure is include in the alarm's additional info.

The procedure names involved are either the configured Diameter request and answer event handler names (**Main Menu > 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**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DCA   |
| <b>Description</b>        | The U-SBR DB logical name could not be resolved to a physical U-SBR DB.   |
| <b>Severity</b>           | Critical  |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalld.shortName</i> ) prefixed with "DCA:" |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | 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

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | DCA  |
| <b>Description</b>      | Diameter message routing failure due to full DRL queue. Diameter egress message could not be sent because the DRL queue is full. |
| <b>Severity</b>         | Info   |
| <b>Instance</b>         | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:"  |
| <b>HA Score</b>         | Normal   |
| <b>Throttle Seconds</b> | 60   |
| <b>OID</b>              | dcaEgressMsgRouteFailureDueToDrlQueueExhaustedNotify   |

#### Recovery

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 33308 - DCA to U-SBR ComAgent Error

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DCA   |
| <b>Description</b>      | DCA failed to send query to U-SBR due to ComAgent Error.                  |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:" |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 60  |
| <b>OID</b>              | dcaComAgentSendFailureNotify  |

#### Recovery

It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

### 33309 - DCA Script Compilation Error

|                    |  |
|--------------------|--|
| <b>Alarm Group</b> | DCA                                      |
| <b>Description</b> | The script generates compilation errors. |
| <b>Severity</b>    | Critical                                 |

|                           |   |
|---------------------------|---|
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:" |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | dcaDSRAppCompileErrorNotify   |

**Recovery**

The error message generated by the Perl interpreter is included in the alarm's additional info.

Fix the error accordingly and recompile the Perl script, or replace the Trial/Production version (depending on whether the DA-MP is a Trial DA-MP or not) with another script version.

**33310 - U-SBR Sub-resource Unavailable**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DCA   |
| <b>Description</b>        | One or more U-SBR server groups hosting a U-SBR DB are unavailable.   |
| <b>Severity</b>           | Major, Critical   |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:" and the U-SBR DB logical name ( <i>DcaLogicalSbr.logSbrDb</i> ) |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | dcaDSRSubresourceUnavailableNotify  |

**Recovery**

1. Monitor U-SBR resources at **Main Menu > Configuration > Resource Domains**.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**33311 - DCA Application Reloaded**

|                         |   |
|-------------------------|---|
| <b>Event Type</b>       | DCA   |
| <b>Description</b>      | The DCA application script has been successfully re-compiled and re-loaded. |
| <b>Severity</b>         | Info  |
| <b>Instance</b>         | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:"   |
| <b>HA Score</b>         | Normal  |
| <b>Throttle Seconds</b> | 0 (zero)  |
| <b>OID</b>              | dcaDcaAppReloadedNotify   |

**Recovery**

No action required.

**33312 - DCA Script Generation Error**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DCA   |
| <b>Description</b>        | The script could not be saved in the /tmp/appworks_temp directory.        |
| <b>Severity</b>           | Critical  |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:" |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 0 (zero)  |
| <b>OID</b>                | dcaDSRAppScriptGenerationErrorNotify                                      |

**Recovery**

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**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DCA   |
| <b>Description</b>        | No mapping has been provisioned for the U-SBR logical name.   |
| <b>Severity</b>           | Critical  |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:" and thread pool (Request, Answer, or SBR Event) |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | 60  |
| <b>OID</b>                | dcaDSRUsbrLogicalNameErrorNotify  |

**Recovery**

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**

|                    |     |
|--------------------|-----|
| <b>Alarm Group</b> | DCA |
|--------------------|-----|

|                           |  |
|---------------------------|--|
| <b>Description</b>        | The differentiation, un-differentiation, or update process of a Custom MEAL has been interrupted and will be retried in 10 seconds |
| <b>Severity</b>           | Minor  |
| <b>Instance</b>           | The DCA App short name ( <i>DcaDalId.shortName</i> ) prefixed with "DCA:"  |
| <b>HA Score</b>           | Normal   |
| <b>Auto Clear Seconds</b> | 0 (zero)   |
| <b>OID</b>                | DcaCustomMealDiffErrorNotification   |

**Recovery**

If the alarm does not clear on its own, it is recommended to contact [My Oracle Support \(MOS\)](#) for assistance.

**DCA Custom MEAL Event Templates****33330-33429 - *DcaCustomMeal.name* + "Alrm"**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DCA   |
| <b>Description</b>        | <i>DcaCustomMeal.descr</i>  |
| <b>Severity</b>           | Minor, Major, Critical  |
| <b>Instance</b>           | "DCA:" concatenated with the <i>DcaDalId.shortName</i>                |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | <i>DcaCustomMeal.autoClearSecs</i> (300 by default)                   |
| <b>OID</b>                | "DcaCustomNotification" concatenated with the <i>DcaCustomMeal.id</i> |

**33430-33479 - *DcaCustomMeal.name* + "Alrm"**

|                           |   |
|---------------------------|---|
| <b>Alarm Group</b>        | DCA   |
| <b>Description</b>        | <i>DcaCustomMeal.descr</i>  |
| <b>Severity</b>           | Minor, Major, Critical  |
| <b>Instance</b>           | "DCA:" concatenated with the <i>DcaDalId.shortName</i>                |
| <b>HA Score</b>           | Normal  |
| <b>Auto Clear Seconds</b> | <i>DcaCustomMeal.autoClearSecs</i> (300 by default)                   |
| <b>OID</b>                | "DcaCustomNotification" concatenated with the <i>DcaCustomMeal.id</i> |

## Independent SBR Alarms and Events (33730-33830)

### 33730 - U-SBR Database Audit Statistics Report

|                         |  |
|-------------------------|--|
| <b>Event Type</b>       | I-SBR                                  |
| <b>Description</b>      | U-SBR Database Audit Statistics Report |
| <b>Severity</b>         | Info                                   |
| <b>Instance</b>         | <SbrSgName>                            |
| <b>HA Score</b>         | Normal                                 |
| <b>Throttle Seconds</b> | 0 (zero)                               |
| <b>OID</b>              | uSBRAuditStatisticsReport              |

#### Recovery

This report provides statistics related to Universal SBR table audits. Each SBR server generates this event upon reaching the last record in a table. The statistics reported are appropriate for the type of table being audited.

# Chapter 5

## Key Performance Indicators (KPIs)

---

### Topics:

- [General KPIs information.....438](#)
- [Computer Aided Policy Making \(CAPM\) KPIs.....441](#)
- [Communication Agent \(ComAgent\) KPIs.....441](#)
- [Diameter \(DIAM\) KPIs.....442](#)
- [DM-IWF KPIs.....442](#)
- [GLA KPIs.....442](#)
- [IDIH KPIs.....443](#)
- [IP Front End \(IPFE\) KPIs.....443](#)
- [MD-IWF KPIs.....444](#)
- [Message Processor \(MP\) KPIs.....444](#)
- [Full Address Based Resolution \(FABR\) KPIs...445](#)
- [Platform KPIs.....445](#)
- [Policy and Charging Application \(PCA\) KPIs.446](#)
- [Range Based Address Resolution \(RBAR\) KPIs.....446](#)
- [Subscriber Binding Repository \(SBR\) KPIs.....447](#)
- [SS7/Sigtran KPIs.....448](#)
- [DCA Framework KPIs.....448](#)
- [DCA Custom MEAL KPIs.....449](#)
- [U-SBR KPIs.....449](#)

This section provides general information about KPIs 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 16: KPIs Server Elements**

| KPIs Status Element | Description  |
|---------------------|--|
| Network Element     | The network element name (set up on the <b>Configuration &gt; Network Elements</b> page) associated with each Server Hostname. |
| Server Hostname     | The server hostname set up on the <b>Configuration &gt; Servers</b> page. All servers in the system are listed here.           |
| Server Indicators:  |  |
| 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.   |

| KPIs Status Element | Description   |
|---------------------|---|
| 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 17: Schedule KPI Data Export Elements**

| Element          | Description  | Data Input Notes   |
|------------------|--|--|
| Export Frequency | Frequency at which the export occurs   | Format: Radio button<br>Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily<br>Default: Once  |
| Task Name        | Name of the scheduled task   | Format: Textbox<br>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<br>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 | Format: Scrolling list<br>Range: 0 to 59   |

| Element     | Description  | Data Input Notes  |
|-------------|--|---|
|             | when the data will be written to the export directory. | Default: 0  |
| Time of Day | Time of day the export occurs                          | Format: Time textbox<br>Range: 15-minute increments<br>Default: 12:00 AM  |
| Day of Week | Day of week on which the export occurs                 | Format: Radio button<br>Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday<br>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**.

The **KPIs** page appears.

2. If necessary, specify filter criteria and click **Go**.  
The KPIs are displayed according to the specified criteria.

3. Click **Export**.  
The **Schedule KPI Data Export** page appears.

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

**Table 18: CAPM KPIs**

| Variable              | Description  |
|-----------------------|--|
| Processing time [ms]  | Average processing time of Rule Template on a per Rule Template basis. |
| Active Templates      | Number of Rule Templates that are in Active state.                     |
| Test Templates        | Number of Rule Templates that are in Test state.                       |
| Development Templates | Number of Rule Templates that are in Development state.                |
| Match Rule            | References one element in the arrayed measurement.                     |

## Communication Agent (ComAgent) KPIs

The KPI values associated with ComAgent are available using **Main Menu > Status & Manage > KPIs**.

**Table 19: 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 20: 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 **Main Menu > Status & Manage > KPIs**

**Table 21: 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. |
| 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.   |

## 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 |

## Key Performance Indicators (KPIs)

| Variable             | Description  |
|----------------------|--|
|                      | 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 **Main Menu > 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 22: 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 23: 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. |

## Key Performance Indicators (KPIs)

| Variable                      | Description  |
|-------------------------------|--|
| Message 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 24: 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 25: Platform KPIs**

| Variable | Description   |
|----------|---|
| CPU      | Percentage utilization of all processors on the server by all software as measured by the operating system. |
| RAM      | Percentage utilization of physical memory on the server by all software as measured by TPD.                 |
| Swap     | Percentage utilization of swap space on the server by all software as measured by TPD.                      |

## Key Performance Indicators (KPIs)

| Variable | Description  |
|----------|--|
| Uptime   | The total amount of time(days HH:MM:SS) the server has been running. |

## Policy and Charging Application (PCA) KPIs

The KPI values associated with PCA are available using **Main Menu > Status & Manage > KPIs**.

**Table 26: 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. |

## Range Based Address Resolution (RBAR) KPIs

The KPI values associated with RBAR are available using **Main Menu > Status & Manage > KPIs**.

**Table 27: 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 **Main Menu > Status & Manage > KPIs**.

**Table 28: SBR KPIs**

| Variable                    | Description                                  |
|-----------------------------|--|
| SBR Memory Utilization      | SBR memory utilization (0-100%)              |
| SBR Process CPU Utilization | SBR Process CPU Percent Utilization (0-100%) |

**Table 29: 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 30: 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 31: SS7/Sigtran KPIs

| Variable                    | Description  |
|-----------------------------|--|
| SCCP Recv Msgs/Sec          | SCCP messages received per second.   |
| SCCP Xmit Msgs/Sec          | SCCP messages transmitted per second.  |
| SS7 Process CPU Utilization | The average percent of SS7 Process CPU utilization on an MP server.  |
| Ingress Message Rate        | The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue. |
| M3RL Xmit Msgs/Sec          | M3RL DATA MSUs/Sec sent.   |
| M3RL Recv Msgs/Sec          | M3RL DATA MSUs/Sec received.   |

## DCA Framework KPIs

The KPI values associated with DCA are visible using **Main Menu > 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   |

## Key Performance Indicators (KPIs)

| Variable                 | Description  |
|--------------------------|--|
| Max Perl Handler Opcodes | Maximum number of opcodes executed by the Perl script event handlers   |
| Opcod 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                   |
|---------------------------|-------------------------------|
| <i>DcaCustomMeal.name</i> | <i>DcaCustomMeal.kpiDescr</i> |

## U-SBR KPIs

The KPI values associated with Universal SBR are visible using **Main Menu > 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 |

## Key Performance Indicators (KPIs)

| Variable                       | Description   |
|--------------------------------|---|
| 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 |

## B

BIOS  
Basic Input-Output System  
Firmware on the CPU blade that is executed prior to executing an OS.

## C

CAPM  
Computer-aided policy making

CCR-I  
CCR Initial

CMOS  
Complementary Metal Oxide Semiconductor  
CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.

ComAgent  
Communication Agent  
A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.

Communication Agent  
See ComAgent.

CPC  
Capability Point Code  
A capability point code used by the SS7 protocol to identify a group of

## C

functionally related STPs in the signaling network.

CSV

Comma-Separated Values

The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

## D

DA-MP

Diameter Agent Message Processor

A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application that can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.

DB

Database

Diameter

Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for

## D

mobility management which is typically associated with an IMS or wireless type of environment.

DM-IWF

Diameter MAP–Interworking  
DSR application that translates Diameter messages into MAP messages.

DNS

Domain Name System  
A system for converting Internet host and domain names into IP addresses.

DP

Data Processor  
The repository of subscriber data on the individual node elements. The DP hosts the full address resolution database.

DPR

Disconnect-Peer-Request  
A message used by a Diameter node to inform its peer of its intent to disconnect the transport layer. Upon receipt of a DPR, the Disconnect-Peer-Answer (DPA) is returned.

DRL

Diameter Routing Layer - The software layer of the stack that implements Diameter routing.

DSR

Diameter Signaling Router  
A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element

## D

may consist of one or more Diameter nodes.

## E

ETG Egress Throttle Group (s)

## F

FABR Full Address Based Resolution  
Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.

FIPS Federal Information Processing Standard

Full Address Based Resolution See FABR.

## G

GGR Get-Gateway-Request  
A request for information for either an IMSI or an MSISDN. Only one subscriber (IMSI or MSISDN) is allowed to be queried per GGR. The GGR is generated by the GQC.

GLA Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B by the Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to

## G

query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.

GQC

Gateway Query Client also known as Diameter Node

GUI

Graphical User Interface

The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

GWS

Gateway Screening

Used at gateway STPs to limit access into the network to authorized users. A gateway STP performs inter-network routing and gateway screening functions. GWS controls access to nonhome SS7 networks. Only an MSU that matches predefined criteria in the EAGLE database is allowed to enter the EAGLE.

## H

HA

High Availability

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

HIDS

Host Intrusion Detection System

HP

Hewlett-Packard

**I**

IDIH Integrated Diameter Intelligence Hub

IPFE IP Front End

A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

**K**

KPI Key Performance Indicator

**L**

LSP Local Signaling Point

A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique primary/true point code within a particular SS7 Domain to an MP server.

**M**

M3RL M3UA Routing Layer

A layer invented by Tekelec to enhance M3UA by adding a true routing layer.

MAP Mobile Application Part

An application part in SS7 signaling for mobile communications systems.

## M

MD-IWF  
MAP-Diameter Interworking SS7 Application, which translates MAP messages into Diameter messages

MP  
Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

MPS  
Messages Per Second  
A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.

## N

NI  
Network Indicator

NOAM  
Network Operations, Administration, and Maintenance

NTP  
Network Time Protocol

NTP daemon  
Network Time Protocol daemon – NTP process that runs in the background.

## O

OAM  
Operations, Administration, and Maintenance. These functions are generally managed by individual applications and not managed by

**O**

a platform management application, such as PM&C.

Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.

Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.

Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).

OID

Object Identifier

An identifier for a managed object in a Management Information Base (MIB) hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB OIDs belong to different standard organizations. Vendors define private branches that include managed objects for their own products.

OOS

Out of Service

OPC

Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.

**P**

PCA

Point Code ANSI

**P**

|      |  |
|------|--|
| PCRF | <p>Policy and Charging Rules Function</p> <p>The ability to dynamically control access, services, network capacity, and charges in a network.</p> <p>Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.</p> <p>In the Policy Management system, PCRF is located in the MPE device.</p> <p>Software node designated in real-time to determine policy rules in a multimedia network.</p> |
| PDU  | Protocol Data Unit   |
| Perl | An object-oriented, event-driven programming language.   |
| PTR  | Pending Transaction Record   |

**R**

|                                |   |
|--------------------------------|---|
| Range Based Address Resolution | See RBAR.   |
| RBAR                           | <p>Range Based Address Resolution</p> <p>A DSR enhanced routing application which allows you to route Diameter end-to-end transactions based on Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges.</p> |

## R

**Relay Agent**

Diameter agent that forwards requests and responses to other Diameter nodes based on routing-related AVPs (such as Destination-Realm) and routing configuration. Because relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type.

**RSP**

Remote Signaling Point

A logical element that represents a unique point code within a particular SS7 domain with which the SS7 application's Local Signaling Point interacts.

## S

**SNMP**

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

**SOAM**

System Operations,  
Administration, and Maintenance

**SOAP**

Simple Object Access Protocol

## S

STP  
Signal Transfer Point  
The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.

SW  
Software

## T

TFA  
TransFer Allowed (Msg)

TFC  
TransFer Controlled (Msg)

TFP  
TransFer Prohibited (Msg)  
A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.

TFR  
Transfer Restricted

TPC  
True Point Code

TSA  
Target Set Address  
An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.