# Table of Contents

## Chapter 1: Introduction
- Overview .................................................................................................................. 54
- Scope and Audience .................................................................................................. 55
- Manual Organization ............................................................................................... 55
- Documentation Admonishments ........................................................................... 55
- Related Publications ............................................................................................... 56
- My Oracle Support (MOS) ...................................................................................... 56
- Emergency Response .............................................................................................. 57
- Locate Product Documentation on the Oracle Technology Network Site .......... 57

## Chapter 2: Alarms and Events, KPIs, and Measurements

### Overview
- Alarms Warning ..................................................................................................... 59
- Displaying the file list ........................................................................................... 60
- Data Export ............................................................................................................. 60
  - Data Export elements .......................................................................................... 60
  - Configuring data export ................................................................................. 62
- Tasks ......................................................................................................................... 63
  - Active Tasks ........................................................................................................ 63
  - Scheduled Tasks ................................................................................................ 66

## Chapter 3: Alarms and Events

- General alarms and events information ................................................................. 69
  - Alarms and events overview .............................................................................. 71
  - Alarms formatting information ........................................................................ 73
  - Alarm and event ID ranges .............................................................................. 73
  - Alarm and event types ...................................................................................... 74
  - Viewing active alarms ..................................................................................... 76
  - Active alarms data export elements ................................................................. 76
  - Exporting active alarms .................................................................................. 77
  - Generating a report of active alarms ............................................................... 78
  - Viewing alarm and event history .................................................................... 79
Historical events data export elements .................................................................79
Exporting alarm and event history .................................................................80
Generating a report of historical alarms and events .....................................81

IP Front End, IPFE (5000-5999) .................................................................82
5000 - IPFE Process Failure .................................................................82
5001 - IPFE Backend Unavailable .................................................................82
5002 - IPFE address configuration error .....................................................82
5003 - IPFE state sync run error .................................................................83
5004 - IPFE IP tables configuration error ...................................................84
5005 - IPFE Backend In Stasis .................................................................84
5006 - Error reading from Ethernet device. Restart IPFE process .............85
5007 - Out of Balance: Low .................................................................85
5008 - Out of Balance: High .................................................................86
5009 - No available servers in target set .....................................................86
5010 - Unknown Linux iptables command error .........................................87
5011 - System or platform error prohibiting operation ...............................87
5012 - Signaling interface heartbeat timeout ...........................................88
5013 - Throttling traffic .................................................................88
5100 - Traffic overload .................................................................89
5101 - CPU Overload .................................................................89
5102 - Disk Becoming Full .................................................................90
5103 - Memory Overload .................................................................90

OAM (10000-10999) .........................................................................................90
10000 - Incompatible database version ....................................................90
10001 - Database backup started .............................................................91
10002 - Database backup completed .......................................................91
10003 - Database backup failed ..............................................................91
10004 - Database restoration started .......................................................92
10005 - Database restoration completed ................................................92
10006 - Database restoration failed .......................................................92
10008 - Database provisioning manually disabled .....................................93
10009 - Config and Prov db not yet synchronized .....................................93
10010 - Stateful db from mate not yet synchronized ....................................93
10011 - Cannot monitor table ...............................................................94
10012 - Table change responder failed ....................................................94
10013 - Application restart in progress ....................................................94
10020 - Backup failure ........................................................................95
10050 - Resource Audit Failure ..................................................................95
10051 - Route Deployment Failed ............................................................95
10052 - Route discovery failed ...............................................................96
10053 - Route deployment failed - no available device ..............................96
10054 - Device deployment failed.................................................................96
10055 - Device discovery failed.................................................................97
10073 - Server Group Max Allowed HA Role Warning..........................97
10074 - Standby server degraded while mate server stabilizes................98
10075 - Application processes have been manually stopped................98
10078 - Application not restarted on standby server due to disabled failure cleanup mode .................................................................98
10100 - Log export started..........................................................................99
10101 - Log export successful.................................................................99
10102 - Log export failed..........................................................................99
10103 - Log export already in progress....................................................100
10104 - Log export file transfer failed......................................................100
10105 - Log export cancelled - user request...........................................100
10106 - Log export cancelled - duplicate request.................................101
10107 - Log export cancelled - queue full..............................................101
10108 - Duplicate scheduled log export task.........................................102
10109 - Log export queue is full..............................................................102
10150 - Login successful..........................................................................103
10151 - Login failed................................................................................103
10152 - Logout successful.........................................................................103
10153 - Logout successful.........................................................................103
10154 - User Account Disabled..............................................................104
10155 - SAML Login Successful...............................................................104
10156 - SAML Login Failed.....................................................................104
10200 - Remote database reinitialization in progress............................105

IDIH (11500-11549).................................................................................. 105
11500 - Tracing Suspended.......................................................................105
11501 - Trace Throttling Active...............................................................105
11502 - Troubleshooting Trace Started....................................................106
11503 - Troubleshooting Trace Stopped....................................................106
11504 - Invalid DIH IP Address...............................................................106

Session Binding Repository, SBR (12000-12010)....................................107
12003 - SBR Congestion State.................................................................107
12007 - SBR Active Sess Binding Threshold...........................................108
12010 - SBR Proc Term...........................................................................108

SS7/Sigtran Alarms (19200-19299).............................................................109
19200 - RSP/Destination unavailable......................................................109
19201 - RSP/Destination route unavailable..........................................109
19202 - Linkset unavailable.................................................................110
19203 - Link unavailable.......................................................................110
19204 - Preferred route unavailable......................................................111
19205 - TFP received.............................................................................111
19206 - TFA received..........................................................112
19207 - TFR received..........................................................112
19208 - TFC received..........................................................112
19209 - M3RL routing error - invalid DPC..........................113
19210 - M3RL routing error - invalid NI.............................113
19211 - M3RL routing error - invalid SI.............................114
19217 - Node isolated - all links down.................................114
19226 - Timedout waiting for ASP-UP-ACK.........................115
19227 - Received unsolicited ASP-DOWN-ACK.....................115
19229 - Timed out waiting for ASP-ACTIVE-ACK...................116
19230 - Received unsolicited ASP-INACTIVE-ACK..................116
19231 - Received invalid M3UA message............................117
19233 - Failed to send non-DATA message..........................118
19234 - Local link maintenance state change.......................118
19235 - Received M3UA error.............................................119
19240 - Remote SCCP subsystem prohibited.........................120
19241 - SCCP message type unrecognizedSCCP malformed or unsupported message..........................................................120
19242 - SCCP Hop counter violation....................................121
19243 - SCCP routing failure..............................................121
19244 - SCCP routing failure network status.......................122
19245 - SCCP GTT failure...................................................122
19246 - Local SCCP subsystem prohibited..........................123
19248 - SCCP Segmentation Failure.....................................124
19249 - SCCP Reassembly Failure.......................................124
19250 - SS7 process CPU utilization....................................124
19251 - Ingress message rate..............................................125
19252 - PDU buffer pool utilization......................................126
19253 - SCCP stack event queue utilization.........................126
19254 - M3RL stack event queue utilization.........................127
19255 - M3RL network management event queue utilization...127
19256 - M3UA stack event queue utilization.........................128
19258 - SCTP Aggregate Egress queue utilization..................129
19259 - Operation discarded due to local resource limitation...129
19260 - Transaction could not be delivered to remote TCAP peer due to conditions in the network..................................................130
19262 - Operation discarded due to malformed component received from remote TCAP peer..................................................130
19263 - Transaction discarded due to malformed dialogue message received from local TC User..................................................131
19264 - Transaction discarded due to malformed dialogue message from remote TCAP peer ................................................................. 131
19265 - Unexpected event received from local TC User ......................................................................................................................... 132
19266 - Unexpected event received from remote TCAP peer .................................................................................................................. 132
19267 - Dialogue removed by dialogue cleanup timer ......................................................................................................................... 132
19268 - Operation removed by invocation timer expiry ......................................................................................................................... 133
19269 - Dialogue aborted by remote TCAP peer .............................................................................................................................. 134
19270 - Received unsupported TCAP message ............................................................................................................................ 134
19271 - Operation rejected by remote TCAP peer ............................................................................................................................ 135
19272 - TCAP active dialogue utilization ........................................................................................................................................ 135
19273 - TCAP active operation utilization ........................................................................................................................................ 136
19274 - TCAP stack event queue utilization ........................................................................................................................................ 136
19275 - Return error from remote TCAP peer .................................................................................................................................... 137
19276 - SCCP Egress Message Rate .................................................................................................................................................. 137
19281 - TCAP Routing Failure ......................................................................................................................................................... 138

Transport Manager Alarms and Events (19400-19499) .......................................................................................................................... 138
19400 - Transport Down ................................................................................................................................................................. 138
19401 - Failed to configure Transport ............................................................................................................................................... 139
19402 - Failed to connect Transport .............................................................................................................................................. 140
19403 - Received malformed SCTP message (invalid length) ........................................................................................................ 140
19404 - Far-end closed the Transport ............................................................................................................................................... 141
19405 - Transport closed due to lack of response .......................................................................................................................... 141
19406 - Local Transport maintenance state change ....................................................................................................................... 142
19407 - Failed to send Transport DATA Message .......................................................................................................................... 142
19408 - Single Transport Egress-Queue Utilization ........................................................................................................................ 143
19409 - Message Rejected by ACL Filtering ..................................................................................................................................... 144
19410 - Adjacent Node IP Address state change ........................................................................................................................... 144
19411 - SCTP Transport closed due to failure of multihoming validation .......................................................................................... 145
19412 - SCTP Transport Transport Configuration Mismatch .......................................................................................................... 145
19413 - SCTP Transport closed due to unsupported peer type evenet recieved ........................................................................ 145

Communication Agent, ComAgent (19800-19909) ............................................................................................................................... 146
19800 - Communication Agent Connection Down .......................................................................................................................... 146
19801 - Communication Agent Connection Locally Blocked ......................................................................................................... 147
19802 - Communication Agent Connection Remotely Blocked .................................................................................................... 148
19803 - Communication Agent stack event queue utilization .................................................................................................... 148
19804 - Communication Agent configured connection waiting for remote client to establish connection .............................................................................................................................................. 149
19805 - Communication Agent Failed To Align Connection ........................................................................................................ 150
19806 - Communication Agent CommMessage mempool utilization ........................................................................................................ 151
19807 - Communication Agent User Data FIFO Queue utilization ................................................................................................... 152
19808 - Communication Agent Connection FIFO Queue utilization .................................................................................................. 152
19810 - Communication Agent Egress Message Discarded.............................................153
19811 - Communication Agent Ingress Message Discarded............................................154
19814 - Communication Agent Peer has not responded to heartbeat............................154
19816 - Communication Agent Connection State Changed.............................................155
19817 - Communication Agent DB Responder detected a change in configurable
         control option parameter.................................................................................................155
19818 - Communication Agent DataEvent Mempool utilization....................................156
19820 - Communication Agent Routed Service Unavailable...........................................156
19821 - Communication Agent Routed Service Degraded..............................................157
19822 - Communication Agent Routed Service Congested.............................................157
19823 - Communication Agent Routed Service Using Low-Priority Connection
         Group.................................................................................................................................158
19824 - Communication Agent Pending Transaction Utilization...................................158
19825 - Communication Agent Transaction Failure Rate.................................................159
19826 - Communication Agent Connection Congested....................................................159
19830 - Communication Agent Service Registration State Change................................160
19831 - Communication Agent Service Operational State Changed..............................161
19832 - Communication Agent Reliable Transaction Failed............................................161
19833 - Communication Agent Service Egress Message Discarded...............................162
19842 - Communication Agent Resource-Provider Registered.......................................162
19843 - Communication Agent Resource-Provider Resource State Changed..............162
19844 - Communication Agent Resource-Provider Stale Status Received....................163
19845 - Communication Agent Resource-Provider Deregistered...................................163
19846 - Communication Agent Resource Degraded.........................................................163
19847 - Communication Agent Resource Unavailable.....................................................164
19848 - Communication Agent Resource Error.................................................................165
19850 - Communication Agent Resource-User Registered..........................................165
19851 - Communication Agent Resource-User Deregistered.........................................165
19852 - Communication Agent Resource Routing State Changed..................................166
19853 - Communication Agent Resource Egress Message Discarded............................166
19854 - Communication Agent Resource-Provider Tracking Table Audit Results
         .............................................................................................................................................166
19855 - Communication Agent Resource Has Multiple Actives......................................166
19856 - Communication Agent Service Provider Registration State Changed.............167
19857 - Communication Agent Service Provider Operational State Changed..............168
19863 - Communication Agent Max Connections Limit In Connection Group
         Reached..............................................................................................................................168
19860 - Communication Agent Configuration Daemon Table Monitoring Failure....168
19861 - Communication Agent Configuration Daemon Script Failure..........................169
19862 - Communication Agent Ingress Stack Event Rate.................................................170
19863 - Communication Agent Max Connections Limit In Connection Group Reached..............................................................................................................................170
19864 - ComAgent Successfully Set Host Server Hardware Profile..............................................................................................................................171
19865 - ComAgent Failed to Set Host Server Hardware Profile ..............................................................................................................................171
19900 - Process CPU Utilization..............................................................................................................................171
19901 - CFG-DB Validation Error..............................................................................................................................172
19902 - CFG-DB Update Failure..............................................................................................................................172
19903 - CFG-DB post-update Error..............................................................................................................................173
19904 - CFG-DB post-update Failure..............................................................................................................................173
19905 - Measurement Initialization Failure..............................................................................................................................174

Diameter Signaling Router (DSR) Diagnostics (19910-19999)..............................................................................................................................174
19910 - Message Discarded at Test Connection..............................................................................................................................174
19911 - Test message discarded..............................................................................................................................................................................................175

Diameter Alarms and Events (22000-22350, 22900-22999)..............................................................................................................................175
22001 - Message Decoding Failure..............................................................................................................................................................................................175
22002 - Peer Routing Rules with Same Priority..............................................................................................................................176
22003 - Application ID Mismatch with Peer..............................................................................................................................176
22004 - Maximum pending transactions allowed exceeded..............................................................................................................................177
22005 - No peer routing rule found..............................................................................................................................................................................................177
22006 - Forwarding Loop Detected..............................................................................................................................................................................................178
22007 - Inconsistent Application ID Lists from a Peer..............................................................................................................................178
22008 - Orphan Answer Response Received..............................................................................................................................................................................................179
22009 - Application Routing Rules with Same Priority..............................................................................................................................................................................................179
22100 - Specified DAS Route List not provisioned..............................................................................................................................................................................................180
22102 - Specified MCCS not provisioned..............................................................................................................................................................................................180
22103 - DAS Peer Number of Retransmits Exceeded for Copy..............................................................................................................................................................................................180
22104 - No DAS Route List specified..............................................................................................................................................................................................181
22105 - Connection Operational Status Inconsistency May Exist..............................................................................................................................................................................................181
22106 - Peer Node Alarm Aggregation Threshold..............................................................................................................................................................................................182
22107 - Route List Alarm Aggregation Threshold..............................................................................................................................................................................................182
22108 - Maintenance Leader HA Notification to go Active..............................................................................................................................................................................................183
22109 - Maintenance Leader HA Notification to go OOS..............................................................................................................................................................................................183
22110 - Copy Message size exceeded the system limit ..............................................................................................................................................................................................183
22111 - Debug Routing Info AVP Enabled..............................................................................................................................................................................................184
22112 - Peer Unavailable..............................................................................................................................................................................................184
22113 - Peer Degraded..............................................................................................................................................................................................185
22114 - Route List Unavailable..............................................................................................................................................................................................185
22115 - Route List Degraded..............................................................................................................................................................................................186
22116 - Non-Preferred Route Group in Use..............................................................................................................................................................................................186
22117 - Egress Throttle Group Rate Limit Degraded..............................................................................................................................................................................................187
22118 - Egress Throttle Group Pending Transaction Limit Degraded..............................................................................................................................................................................................187
22059 - Egress Throttle Group Message Rate Congestion Level changed.....................188
22060 - Egress Throttle Group Pending Transaction Limit Congestion Level
changed..............................................................................................................................189
22061 - Egress Throttle Group Monitoring stopped.........................................................189
22062 - Actual Host Name cannot be determined for Topology Hiding.......................190
22063 - Diameter Max Message Size Limit Exceeded.......................................................190
22101 - Connection Unavailable...........................................................................................190
22102 - Connection Degraded..............................................................................................191
22103 - SCTP Connection Impaired.....................................................................................191
22104 - SCTP peer is operating with a reduced IP address set........................................192
22106 - Ingress Message Discarded: DA-MP Ingress Message Rate Control..............192
22200 - Local MP Congestion...............................................................................................193
22201 - Ingress Message Rate...............................................................................................193
22202 - PDU Buffer Pool Utilization....................................................................................194
22203 - PTR Buffer Pool Utilization.....................................................................................194
22204 - Request Message Queue Utilization......................................................................195
22205 - Answer Message Queue Utilization........................................................................196
22206 - Reroute Queue Utilization.......................................................................................196
22207 - All-Connections Event Queue Utilization.............................................................197
22208 - Per-Connection Egress Message Queue Utilization............................................197
22209 - Message Copy Disabled...........................................................................................198
22214 - Message Copy Queue Utilization...........................................................................198
22215 - Ingress Message Discarded: DA-MP Overload Control.....................................199
22216 - Ingress Message Discarded: Priority 0 message discarded by DA-MP
Overload Control................................................................................................................199
22217 - Ingress Message Discarded: Priority 1 message discarded by DA-MP
Overload Control................................................................................................................200
22218 - Ingress Message Discarded: Priority 2 message discarded by DA-MP
Overload Control................................................................................................................200
22220 - Connection Congestion Level change....................................................................201
22221 - Routing MPS Rate ....................................................................................................202
22222 - Long Timeout PTR Buffer Pool Utilization...........................................................203
22223 - DA-MP Memory Utilization Exceeded..................................................................203
22224 - Average Hold Time Limit Exceeded......................................................................204
22225 - Average Message Size Limit Exceeded.................................................................204
22300 - Connection Unavailable: Socket configuration failure........................................205
22301 - Connection Unavailable: Connection initiation failure......................................205
22302 - Connection Unavailable: Received malformed message....................................205
22303 - Connection Unavailable: Peer closed connection..............................................206
22304 - Connection Unavailable: Proving Failure............................................................206
22305 - Connection Admin State change............................................................................207
22306 - Connection Unavailable: Timeout waiting for CER/CEA ................................207
22307 - Connection Unavailable: Timeout waiting for DPA........................................207
22308 - Received Unexpected CER/CEA.....................................................................208
22309 - Received Unexpected DWR/DWA....................................................................208
22310 - Received Unexpected DPR/DPA.....................................................................208
22311 - Invalid Diameter message received..................................................................209
22312 - Socket send failure............................................................................................209
22313 - Connection Unavailable: Transport failure.......................................................210
22314 - Connection Unavailable: CEA Realm/Host validation failure.........................210
22315 - Connection Unavailable: Peer IP address validation failure............................210
22316 - Connection Unavailable: No common apps......................................................211
22317 - Connection Rejected: Connection already established......................................211
22318 - Connection Rejected: Connection not Enabled................................................211
22319 - Connection Unavailable: Diameter Watchdog................................................212
22320 - Invalid peer initiated connection......................................................................212
22321 - Connection Unavailable: DNS Resolution Failure...........................................213
22322 - Connection Proving Success............................................................................213
22324 - Connection Unavailable: CER validation failure.............................................213
22325 - Host-IP-Address AVP(s) in CER/CEA do not match peer IP address(es)..........214
22326 - Connection Established....................................................................................214
22327 - Initiator function disabled..................................................................................215
22328 - Connection is processing a higher than normal ingress messaging rate.............215
22329 - SCTP Connection Impaired: A path has become unreachable.........................216
22330 - SCTP Connection Cfg Mismatch: The peer advertised a different number of IP addresses than configured.................................................................216
22331 - SCTP Connection Partial Matching: SCTP connection accepted but the IP addresses advertised by the peer match only partially those configured for the peer in the connection object.........................................................217
22332 - Connection Rejected: Max Connections Exceeded...........................................217
22333 - Connection Rejected: Insufficient Ingress MPS..............................................218
22334 - Unexpected Message Priority in ingress Request..............................................218
22335 - Peer does not support Message Priority............................................................219
22336 - Connection Rejected: Multithomed SCTP connection attempt........................219
22343 - Connection Unavailable: Duplicate Connection Released..............................220
22344 - Failed to process ingress message: Processor Unavailable or Congested............220
22345 - Connection Priority Level changed....................................................................220
22346 - MP Reserved Ingress MPS Oversubscribed.......................................................221
22347 - Ingress Message Discarded: DA-MP shared ingress capacity exhausted..........221
22349 - IPFE Connection Alarm Aggregation Threshold...............................................222
22350 - Fixed Connection Alarm Aggregation Threshold...............................................222
22900 - DPI DB Table Monitoring Overrun...................................................................223
22901 - DPI DB Table Monitoring Error ................................................................. 223
22950 - Connection Status Inconsistency Exists .................................................... 224
22960 - DA-MP Profile Not Assigned .................................................................. 224
22961 - Insufficient Memory for Feature Set ........................................................ 224

Range Based Address Resolution (RBAR) Alarms and Events (22400-22424) .......... 225
22400 - Message Decoding Failure ....................................................................... 225
22401 - Unknown Application ID .......................................................................... 225
22402 - Unknown Command Code ........................................................................ 226
22403 - No Routing Entity Address AVPs ............................................................... 226
22404 - No valid Routing Entity Addresses found ................................................. 227
22405 - Valid address received didn’t match a provisioned address or address range ................................................................. 227
22406 - Routing attempt failed due to internal resource exhaustion ....................... 227
22407 - Routing attempt failed due to internal database inconsistency failure ........ 228

Generic Application Alarms and Events (22500-22599) .......................................... 228
22500 - DSR Application Unavailable .................................................................. 228
22501 - DSR Application Degraded ...................................................................... 229
22502 - DSR Application Request Message Queue Utilization ............................. 230
22503 - DSR Application Answer Message Queue Utilization .............................. 230
22504 - DSR Application Ingress Message Rate ................................................... 231
25510 - Multiple DA-MP Leader Detected Alarm .................................................. 232
22520 - DSR Application Enabled ......................................................................... 232
22521 - DSR Application Disabled ....................................................................... 232

Full Address Based Resolution (FABR) Alarms and Events (22600-22640) ............ 233
22600 - Message Decoding Failure ....................................................................... 233
22601 - Unknown Application ID .......................................................................... 233
22602 - Unknown Command Code ....................................................................... 234
22603 - No Routing Entity Address AVPs ............................................................... 234
22604 - No valid User Identity Addresses found ................................................... 235
22605 - No Destination address is found to match the valid User Identity address ................................................................................. 235
22606 - Database or DB connection error ............................................................... 236
22607 - Routing attempt failed due to DRL queue exhaustion ............................... 236
22608 - Database query could not be sent due to DB congestion ......................... 236
22609 - Database connection exhausted .............................................................. 237
22610 - FABR DP Service congestion state change ............................................... 237
22611 - FABR Blacklisted Subscriber .................................................................... 237
22631 - FABR DP Response Task Message Queue Utilization ............................. 238
22632 - COM Agent Registration Failure ............................................................ 238

Policy DRA (PDRA) Alarms and Events (22700-22799) ............................................ 239
22700 - Protocol errors in Diameter Requests ....................................................... 239
22701 - Protocol errors in Diameter Answers.................................................................239
22702 - Database Hash Function Error.................................................................239
22703 - Diameter message routing failure due to DRL queue exhaustion ........240
22704 - Policy DRA Communication Agent Error.................................................240
22705 - Policy SBR Error Response Received By Policy DRA.................................240
22706 - Binding Key Not Found In Diameter Message...........................................241
22707 - Policy DRA Diameter Message Processing Failure.................................241
22710 - Policy SBR Sessions Threshold Exceeded..................................................241
22711 - Policy SBR Database Error...........................................................................242
22712 - Policy SBR Communication Error..............................................................242
22713 - Policy SBR Alternate Key Creation Error....................................................243
22714 - Policy SBR RAR Initiation Error.................................................................243
22715 - Policy SBR Audit Suspended.......................................................................243
22716 - Policy SBR Audit Statistics Report.............................................................244
22717 - Policy SBR Alternate Key Creation Failure Rate..........................................244
22718 - Binding Not Found for Binding Dependent Session Initiate Request........245
22719 - Maximum Number of Sessions per Binding Exceeded............................245
22720 - Policy SBR To Policy DRA Response Queue Utilization Threshold
     Exceeded..................................................................................................................246
22721 - Policy DRA Server In Congestion...............................................................246
22722 - Policy DRA Binding Sub-resource Unavailable ........................................247
22723 - Policy DRA Session Sub-resource Unavailable..........................................247
22724 - Policy SBR Memory Utilization Threshold Exceeded...............................248
22725 - Policy SBR Server In Congestion...............................................................248
22726 - Policy SBR Queue Utilization Threshold Exceeded....................................249
22727 - Policy SBR Initialization Failure.................................................................249
22728 - Policy SBR Bindings Threshold Exceeded..................................................249
22729 - PCRF Not Configured...................................................................................250
22730 - Policy DRA Configuration Error...............................................................250
22731 - Policy DRA Database Inconsistency............................................................251
22732 - Policy SBR Process CPU Utilization Threshold Exceeded.......................251
22733 - Policy SBR Failed to Free Binding Memory After PCRF Pooling Binding
     Migration....................................................................................................................252
22734 - Policy DRA Unexpected Stack Event Version............................................252
22735 - Policy DRA session initiation request received with no APN....................253
Charging Proxy Application (CPA) Alarms and Events (22800-22849)................254
22804 - Number of cSBR Unavailable Subresources at Threshold.......................254
22805 - Message Decoding Failure.......................................................................254
22806 - Unknown Diameter Application Id............................................................255
22807 - Unknown Command Code........................................................................255
22808 - Session Not Found......................................................................................255
22809 - Undelivered SBR Query

22810 - Routing attempt failed due to internal resource exhaustion

22811 - CPA Application Event Task Queue Utilization

22812 - Missing AVP

22813 - Received an error response to an SBR Query

22814 - HA Sub-Resource Unavailable

22815 - Unexpected Session

22816 - One or more cSBR Subresources Unavailable

Tekelec Virtual Operating Environment, TVOE (24400-24499)

24400 - TVOE libvirtd is down

24401 - TVOE libvirtd is hung

24402 - all TVOE libvirtd connections are in use

Computer Aided Policy Making, CAPM (25000-25499)

25000 - Rule Template failed to be updated

25001 - Action failed within the Rule Template

25002 - Stop Rule Template processing after action failure

25003 - Exit Trigger point after action failure

OAM Alarm Management (25500-25899)

25500 - No DA-MP Leader Detected Alarm

25510 - Multiple DA-MP Leader Detected Alarm

Platform (31000-32700)

Alarms formatting information

31000 - S/W fault

31001 - S/W status

31002 - Process watchdog failure

31003 - Tab thread watchdog failure

31100 - Database replication fault

31101 - Database replication to slave failure

31102 - Database replication from master failure

31103 - DB Replication update fault

31104 - DB Replication latency over threshold

31105 - Database merge fault

31106 - Database merge to parent failure

31107 - Database merge from child failure

31108 - Database merge latency over threshold

31109 - Topology config error

31110 - Database audit fault

31111 - Database merge audit in progress

31112 - Stateful db synchronization from mate server

31113 - DB replication manually disabled

31114 - DB replication over SOAP has failed
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31115</td>
<td>Database service fault</td>
</tr>
<tr>
<td>31116</td>
<td>Excessive shared memory</td>
</tr>
<tr>
<td>31117</td>
<td>Low disk free</td>
</tr>
<tr>
<td>31118</td>
<td>Database disk store fault</td>
</tr>
<tr>
<td>31119</td>
<td>Database updatelog overrun</td>
</tr>
<tr>
<td>31120</td>
<td>Database updatelog write fault</td>
</tr>
<tr>
<td>31121</td>
<td>Low disk free early warning</td>
</tr>
<tr>
<td>31122</td>
<td>Excessive shared memory early warning</td>
</tr>
<tr>
<td>31123</td>
<td>Database replication audit command complete</td>
</tr>
<tr>
<td>31124</td>
<td>ADIC error</td>
</tr>
<tr>
<td>31125</td>
<td>Database durability degraded</td>
</tr>
<tr>
<td>31126</td>
<td>Audit blocked</td>
</tr>
<tr>
<td>31127</td>
<td>DB Replication Audit Complete</td>
</tr>
<tr>
<td>31128</td>
<td>ADIC Found Error</td>
</tr>
<tr>
<td>31129</td>
<td>ADIC Found Minor Issue</td>
</tr>
<tr>
<td>31130</td>
<td>Network health warning</td>
</tr>
<tr>
<td>31131</td>
<td>IDB Throttled for Extended Period</td>
</tr>
<tr>
<td>31140</td>
<td>Database perl fault</td>
</tr>
<tr>
<td>31145</td>
<td>Database SQL fault</td>
</tr>
<tr>
<td>31146</td>
<td>DB mastership fault</td>
</tr>
<tr>
<td>31147</td>
<td>DB upsynclog overrun</td>
</tr>
<tr>
<td>31148</td>
<td>DB lock error detected</td>
</tr>
<tr>
<td>31200</td>
<td>Process management fault</td>
</tr>
<tr>
<td>31201</td>
<td>Process not running</td>
</tr>
<tr>
<td>31202</td>
<td>Unkillable zombie process</td>
</tr>
<tr>
<td>31206</td>
<td>Process mgmt monitoring fault</td>
</tr>
<tr>
<td>31207</td>
<td>Process resource monitoring fault</td>
</tr>
<tr>
<td>31208</td>
<td>IP port server fault</td>
</tr>
<tr>
<td>31209</td>
<td>Hostname lookup failed</td>
</tr>
<tr>
<td>31213</td>
<td>Process scheduler fault</td>
</tr>
<tr>
<td>31214</td>
<td>Scheduled process fault</td>
</tr>
<tr>
<td>31215</td>
<td>Process resources exceeded</td>
</tr>
<tr>
<td>31216</td>
<td>SysMetric configuration error</td>
</tr>
<tr>
<td>31220</td>
<td>HA configuration monitor fault</td>
</tr>
<tr>
<td>31221</td>
<td>HA alarm monitor fault</td>
</tr>
<tr>
<td>31222</td>
<td>HA not configured</td>
</tr>
<tr>
<td>31223</td>
<td>HA Heartbeat transmit failure</td>
</tr>
<tr>
<td>31224</td>
<td>HA configuration error</td>
</tr>
<tr>
<td>31225</td>
<td>HA service start failure</td>
</tr>
<tr>
<td>31226</td>
<td>HA availability status degraded</td>
</tr>
<tr>
<td>31227</td>
<td>HA availability status failed</td>
</tr>
</tbody>
</table>
31228 - HA standby offline...................................................................................................283
31229 - HA score changed.....................................................................................................283
31230 - Recent alarm processing fault................................................................................283
31231 - Platform alarm agent fault.......................................................................................284
31232 - Late heartbeat warning............................................................................................284
31233 - HA Secondary Path Down......................................................................................284
31234 - Untrusted Time Upon Initialization......................................................................285
31235 - Untrusted Time After Initialization......................................................................285
31236 - HA Link Down..........................................................................................................285
31240 - Measurements collection fault................................................................................286
31250 - RE port mapping fault..............................................................................................286
31260 - Database SNMP Agent.............................................................................................286
31270 - Logging output..........................................................................................................287
31280 - HA Active to Standby transition............................................................................287
31281 - HA Standby to Active transition............................................................................287
31282 - HA Management Fault............................................................................................288
31283 - HA Server Offline.....................................................................................................288
31284 - HA Remote Subscriber Heartbeat Warning..........................................................288
31285 - HA Split Brain Recovery Entry............................................................................289
31286 - HA Split Brain Recovery Plan..............................................................................289
31287 - HA Split Brain Recovery Complete.......................................................................289
31290 - HA Process Status.....................................................................................................290
31291 - HA Election Status..................................................................................................290
31292 - HA Policy Status......................................................................................................290
31293 - HA Resource Link Status.......................................................................................291
31294 - HA Resource Status................................................................................................291
31295 - HA Action Status.....................................................................................................291
31296 - HA Monitor Status...................................................................................................292
31297 - HA Resource Agent Info.......................................................................................292
31298 - HA Resource Agent Detail....................................................................................292
31299 - HA Notification Status..........................................................................................293
31300 - HA Control Status..................................................................................................293
32100 - Breaker Panel Feed Unavailable..........................................................................293
32101 - Breaker Panel Breaker Failure.............................................................................294
32102 - Breaker Panel Maint Failure..................................................................................294
32103 - Power Feed Unavailable........................................................................................294
32104 - Power Supply 1 Failure..........................................................................................294
32105 - Power Supply 2 Failure..........................................................................................295
32106 - Power Supply 3 Failure..........................................................................................295
32107 - Raid Feed Unavailable............................................................................................295
32108 - Raid Power 1 Failure..............................................................................................296
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32109</td>
<td>Raid Power 2 Failure</td>
</tr>
<tr>
<td>32110</td>
<td>Raid Power 3 Failure</td>
</tr>
<tr>
<td>32111</td>
<td>Device Failure</td>
</tr>
<tr>
<td>32112</td>
<td>Device Interface Failure</td>
</tr>
<tr>
<td>32113</td>
<td>Uncorrectable ECC memory error</td>
</tr>
<tr>
<td>32114</td>
<td>SNMP get failure</td>
</tr>
<tr>
<td>32115</td>
<td>TPD NTP Daemon Not Synchronized Failure</td>
</tr>
<tr>
<td>32116</td>
<td>TPD Server's Time Has Gone Backwards</td>
</tr>
<tr>
<td>32117</td>
<td>TPD NTP Offset Check Failure</td>
</tr>
<tr>
<td>32300</td>
<td>Server fan failure</td>
</tr>
<tr>
<td>32301</td>
<td>Server internal disk error</td>
</tr>
<tr>
<td>32302</td>
<td>Server RAID disk error</td>
</tr>
<tr>
<td>32303</td>
<td>Server Platform error</td>
</tr>
<tr>
<td>32304</td>
<td>Server file system error</td>
</tr>
<tr>
<td>32305</td>
<td>Server Platform process error</td>
</tr>
<tr>
<td>32306</td>
<td>Server RAM shortage error</td>
</tr>
<tr>
<td>32307</td>
<td>Server swap space shortage failure</td>
</tr>
<tr>
<td>32308</td>
<td>Server provisioning network error</td>
</tr>
<tr>
<td>32309</td>
<td>Eagle Network A Error</td>
</tr>
<tr>
<td>32310</td>
<td>Eagle Network B Error</td>
</tr>
<tr>
<td>32311</td>
<td>Sync Network Error</td>
</tr>
<tr>
<td>32312</td>
<td>Server disk space shortage error</td>
</tr>
<tr>
<td>32313</td>
<td>Server default route network error</td>
</tr>
<tr>
<td>32314</td>
<td>Server temperature error</td>
</tr>
<tr>
<td>32315</td>
<td>Server mainboard voltage error</td>
</tr>
<tr>
<td>32316</td>
<td>Server power feed error</td>
</tr>
<tr>
<td>32317</td>
<td>Server disk health test error</td>
</tr>
<tr>
<td>32318</td>
<td>Server disk unavailable error</td>
</tr>
<tr>
<td>32319</td>
<td>Device error</td>
</tr>
<tr>
<td>32320</td>
<td>Device interface error</td>
</tr>
<tr>
<td>32321</td>
<td>Correctable ECC memory error</td>
</tr>
<tr>
<td>32322</td>
<td>Power Supply A error</td>
</tr>
<tr>
<td>32323</td>
<td>Power Supply B error</td>
</tr>
<tr>
<td>32324</td>
<td>Breaker panel feed error</td>
</tr>
<tr>
<td>32325</td>
<td>Breaker panel breaker error</td>
</tr>
<tr>
<td>32326</td>
<td>Breaker panel monitoring error</td>
</tr>
<tr>
<td>32327</td>
<td>Server HA Keepalive error</td>
</tr>
<tr>
<td>32328</td>
<td>DRBD is unavailable</td>
</tr>
<tr>
<td>32329</td>
<td>DRBD is not replicating</td>
</tr>
<tr>
<td>32330</td>
<td>DRBD peer problem</td>
</tr>
<tr>
<td>32331</td>
<td>HP disk problem</td>
</tr>
</tbody>
</table>
32332 – HP Smart Array controller problem..........................................................................................314
32333 – HP hpcucliStatus utility problem..................................................................................................314
32334 - Multipath device access link problem.........................................................................................314
32335 - Switch link down error..................................................................................................................315
32336 – Half Open Socket Limit................................................................................................................315
32337 - E5-APP-B Firmware Flash...........................................................................................................315
32338 - E5-APP-B Serial mezzanine seating............................................................................................316
32339 - Max pid limit..................................................................................................................................316
32340 - Server NTP Daemon Lost Synchronization....................................................................................316
32341 - Server NTP Daemon Never Synchronized Error..........................................................................317
32342 - NTP Offset Check Error...............................................................................................................317
32343 - RAID disk problem.......................................................................................................................318
32344 - RAID controller problem...............................................................................................................318
32345 - Server Upgrade snapshot(s) invalid.............................................................................................318
32500 – Server disk space shortage warning...............................................................................................319
32501 – Server application process error....................................................................................................319
32502 – Server hardware configuration error.............................................................................................320
32503 – Server RAM shortage warning.......................................................................................................320
32504 – Software Configuration Error.........................................................................................................320
32505 – Server swap space shortage warning..............................................................................................321
32506 – Server default router not defined....................................................................................................321
32507 – Server temperature warning..........................................................................................................321
32508 – Server core file detected................................................................................................................322
32509 – Server NTP Daemon not synchronized........................................................................................322
32510 – CMOS battery voltage low.............................................................................................................323
32511 – Server disk self test warning..........................................................................................................323
32512 – Device warning.............................................................................................................................324
32513 – Device interface warning...............................................................................................................324
32514 – Server reboot watchdog initiated....................................................................................................324
32515 – Server HA failover inhibited...........................................................................................................325
32516 – Server HA Active to Standby transition..........................................................................................325
32517 – Server HA Standby to Active transition..........................................................................................325
32518 – Platform Health Check failure.......................................................................................................326
32519 – NTP Offset Check failure...............................................................................................................326
32520 – NTP Stratum Check failure.............................................................................................................327
32521 – SAS Presence Sensor Missing.......................................................................................................327
32522 – SAS Drive Missing..........................................................................................................................327
32523 – DRBD failover busy..........................................................................................................................328
32524 – HP disk resync...............................................................................................................................328
32525 – Telco Fan Warning..........................................................................................................................328
32526 – Telco Temperature Warning...........................................................................................................329
32527 – Telco Power Supply Warning ................................................................. 329
32528 – Invalid BIOS value ................................................................................ 330
32529– Server Kernel Dump File Detected ........................................................... 330
32530– Server Upgrade Fail Detected ................................................................. 330
32531– Half Open Socket Warning ..................................................................... 331
32532– Server Upgrade Pending Accept/Reject ..................................................... 331
32533 - Max pid warning ....................................................................................... 331
32534 - NTP Source Server Is Not Able To Provide Correct Time ......................... 332
32535 - RAID disk resync .................................................................................... 332
32536 - Server Upgrade snapshot(s) warning ....................................................... 332
32700 - Telco Switch snapshot .......................................................................... 333

DM-IWF (33000-33024) ................................................................................... 333
33000 - MAP-to-Diameter Service Registration Failure on DA-MP ..................... 334
33001 - Diameter-to-MAP Service Registration Failure on DA-MP ..................... 334
33002 - DM-IWF DA-MP not associated with a Place .......................................... 334
33003 - Insufficient memory for DM-IWF ......................................................... 335
33004 - DM-IWF Transaction Response Queue Utilization ............................... 335
33005 - DM-IWF PTR Pool Utilization ............................................................... 336
33006 - MD-IWF Service Congestion ............................................................... 336
33007 - MD-IWF Error ....................................................................................... 337
33008 - DM-IWF maximum pending transactions allowed exceeded................ 337
33009 - DM-IWF unexpected Answer response received from a SS7-MP .......... 338
33010 - MD-IWF ComAgent Connection exhausted ......................................... 338
33011 - DM-IWF Answer Timeout ................................................................... 338
33012 - DM-IWF encode decode error .............................................................. 339
33013 - DRL queue exhaustion ...................................................................... 339
33014 - Incompatible DA-MP Profile for DM-IWF .......................................... 340
33015 - DM-IWF Diameter message size exceeded maximum supported size ...... 340

MD-IWF (33050-33099) ............................................................................... 341
33050 - MD-IWF Ingress Message Rate ............................................................. 341
33051 - MD-IWF Application Degraded or Unavailable ..................................... 341
33052 - MD-IWF Notified that DM-IWF Service Status is Down ......................... 342
33053 - MD-IWF DiamTrans Task Queue Utilization ......................................... 343
33054 - MD-IWF MapTrans Task Queue Utilization ......................................... 343
33055 - MD-IWF DAMPInterface Task Queue Utilization ................................. 344
33056 - MD-IWF ComAgent Provider Registration Failure on SS7-MP ............... 344
33057 - MD-IWF ComAgent User Registration Failure on SS7-MP ................... 344
33058 - MD-IWF DiamToMap PTR Utilization ................................................... 345
33059 - MD-IWF MapToDiam PTR Utilization ............................................... 345
33060 - SS7-MP Profile Not Assigned ............................................................... 346
33062 - Insufficient Memory for MD-IWF ....................................................... 346
33063 - MD-IWF SS7-MP not associated with a Place .......................................................... 347
33065 - MD-IWF Resource Exhaustion .............................................................................. 347
33066 - MD-IWF orphan Diameter Answer message received ........................................ 347
33067 - MD-IWF orphan MAP Response message received ............................................. 348
33068 - MD-IWF MAP Response timeout ....................................................................... 348
33069 - MD-IWF Diameter Answer timeout ................................................................... 349
33070 - MD-IWF Generated Diameter Answer error message due to Diameter Exception .......................................................... 349
33071 - MD-IWF Generated MAP Error Response due to MAP exception ...................... 350
33072 - MD-IWF received TCAP Notice from SS7 network ............................................ 350
33073 - MD-IWF admin state set to Enabled .................................................................... 350
33074 - MD-IWF admin state set to Disabled .................................................................. 351
33075 - MD-IWF received ComAgent error or DM-IWF NACK ..................................... 351
33076 - MD-IWF received Diameter Anwer from unexpected DA-MP ......................... 351
33077 - MD-IWF address translation failed .................................................................... 352
33078 - MD-IWF received Diameter EIR message but Destination-Host AVP not present or not found in mapping table ............................................................. 352
33079 - MD-IWF message translation failed .................................................................. 353
33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message .......................................................................................................................... 353

GLA (33100-33149) .............................................................................................................. 353
33100 - GLA Message Decoding Failure ....................................................................... 354
33101 - GLA Incorrect Application ID or Command Code ............................................. 354
33102 - GLA Missing Subscriber ID .............................................................................. 354
33103 - GLA Communication Agent Error ...................................................................... 355
33104 - GLA Duplicate Subscriber ID ............................................................................ 355
33105 - Routing Attempt failed due to queue exhaustion ............................................... 356
33106 - GLA Communication Agent Timeout .................................................................. 356
33120 - Policy SBR Binding Sub-Resource Unavailable ................................................. 357
33121 - GLA pSBR-B Response Task Message Queue Utilization .................................. 357

Chapter 4: Key Performance Indicators (KPIs) ............................................................... 359

General KPIs information ........................................................................................................... 360
KPIs overview .............................................................................................................................. 360
KPIs ......................................................................................................................................... 360
KPIs server elements ................................................................................................................. 360
Viewing KPIs ............................................................................................................................... 361
KPIs data export elements .......................................................................................................... 361
Exporting KPIs .......................................................................................................................... 362
Computer Aided Policy Making (CAPM) KPIs ................................................................. 363
Chapter 5: Measurements..................................................................................372

General measurements information...............................................................375

   Measurements..........................................................................................375

   Measurement elements ............................................................................375

   Generating a measurements report............................................................377

   Measurements data export elements .........................................................377

   Exporting measurements reports..............................................................378

Address Resolution Exception measurements............................................379

   RxRbarDecodeFailureResol........................................................................381

   RxFabrInvalidImsiMcc..............................................................................381

   RxRbarResolFailAll..................................................................................382

   RxRbarResolFailCmdcode.........................................................................382

   RxRbarResolFailDbFail.............................................................................383

   RxRbarResolFailImpiMatch......................................................................383

   RxRbarResolFailImpuMatch......................................................................383

   RxRbarResolFailImsiMatch......................................................................384

   RxRbarResolFailIpv4Match......................................................................384

   RxRbarResolFailIpv6prefixMatch..............................................................385

   RxRbarResolFailMsisdnMatch...................................................................385

   RxRbarResolFailNoAddrAvps....................................................................386

   RxRbarResolFailNoValidAddr.................................................................386

   RxRbarResolFailUnsigned16Match............................................................387

   RxRbarUnkApplId.....................................................................................387
TxRbarAbandonRequest ........................................................................................................388
Address Resolution Performance measurements .........................................................................388
RxRbarAvgMsgRate ................................................................................................................390
RxRbarMsgs ................................................................................................................................390
RxRbarResolAll ......................................................................................................................390
RxRbarResolAllMp ................................................................................................................391
RxRbarResolImpi ...................................................................................................................391
RxRbarResolImpu ..................................................................................................................392
RxRbarResolImsi ....................................................................................................................392
RxRbarResolIpv4 ....................................................................................................................392
RxRbarResolIpv6prefix .........................................................................................................393
RxRbarResolMsisdn ..............................................................................................................393
RxRbarResolRateAvg ............................................................................................................393
RxRbarResolRatePeak ...........................................................................................................393
RxRbarResolSingleAddr .......................................................................................................394
RxRbarResolUnsigned16 .......................................................................................................394
TxRbarFwdDefaultDest ........................................................................................................395
TxRbarFwdNoChange ...........................................................................................................395
TxRbarFwdSuccess ................................................................................................................395
TxRbarMsgAttempt ...............................................................................................................396
Application Routing Rules measurements .....................................................................................396
RxApplRuleSelected ..............................................................................................................397
RxApplRuleFwdFailAll .........................................................................................................397
RxApplRuleFwdFailUnavail ..................................................................................................398
RxApplRuleDuplicatePriority ..............................................................................................398
RxArtSelected .........................................................................................................................399
Association Exception measurements ..........................................................................................399
RxTrFarEndClose ...................................................................................................................400
EvTrManClose .......................................................................................................................401
EvTrNoRespClose ................................................................................................................401
EvTrCnxFail ..........................................................................................................................402
TxTrSendFail ........................................................................................................................403
RxTrRcvFail ..........................................................................................................................403
EvTrSockInitFail ..................................................................................................................404
RxAsnM3uaERROR ...............................................................................................................404
EvAsnUpAckTO .....................................................................................................................405
RxAsnUnsolDownAck ...........................................................................................................405
RxAsnInvalidM3ua ................................................................................................................406
TmSingleTransQueueFull ......................................................................................................406
EvSctpAdjPToDwn ................................................................................................................407
EvSctpTransRej ......................................................................................................................407
<table>
<thead>
<tr>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association Performance measurements</td>
<td>408</td>
</tr>
<tr>
<td>TxTrOctets</td>
<td>409</td>
</tr>
<tr>
<td>RxTrOctets</td>
<td>409</td>
</tr>
<tr>
<td>SCTPAssocQueuePeak</td>
<td>409</td>
</tr>
<tr>
<td>SCTPAssocQueueAvg</td>
<td>410</td>
</tr>
<tr>
<td>Association Usage measurements</td>
<td>410</td>
</tr>
<tr>
<td>EvTrCnxSuccess</td>
<td>411</td>
</tr>
<tr>
<td>TmAsnBlkNotDown</td>
<td>412</td>
</tr>
<tr>
<td>TmAsnEnaNotUp</td>
<td>412</td>
</tr>
<tr>
<td>Charging Proxy Application (CPA) Exception measurements</td>
<td>413</td>
</tr>
<tr>
<td>EvCpaMessageDecodeFail</td>
<td>414</td>
</tr>
<tr>
<td>EvCpaMissingAvp</td>
<td>414</td>
</tr>
<tr>
<td>EvCpaOOS</td>
<td>415</td>
</tr>
<tr>
<td>EvCpaSubResourceCongested</td>
<td>415</td>
</tr>
<tr>
<td>EvCpaUnexpectedSess</td>
<td>415</td>
</tr>
<tr>
<td>EvCpaUnkDiameterAppId</td>
<td>416</td>
</tr>
<tr>
<td>RxCpaHaSubResourceUnavail</td>
<td>416</td>
</tr>
<tr>
<td>RxCpaNon2xxxAnswer</td>
<td>416</td>
</tr>
<tr>
<td>RxCpaOpStatusUnavail</td>
<td>417</td>
</tr>
<tr>
<td>RxCpaUnexpected</td>
<td>417</td>
</tr>
<tr>
<td>TxCpaAnswerByCpa</td>
<td>418</td>
</tr>
<tr>
<td>TxCpaRteFailure</td>
<td>418</td>
</tr>
<tr>
<td>Charging Proxy Application (CPA) Performance measurements</td>
<td>418</td>
</tr>
<tr>
<td>RxCpaAcaEvent</td>
<td>420</td>
</tr>
<tr>
<td>RxCpaAcaInterim</td>
<td>420</td>
</tr>
<tr>
<td>RxCpaAcaStart</td>
<td>421</td>
</tr>
<tr>
<td>RxCpaAcaStop</td>
<td>421</td>
</tr>
<tr>
<td>RxCpaAccounting</td>
<td>421</td>
</tr>
<tr>
<td>RxCpaAcrEvent</td>
<td>422</td>
</tr>
<tr>
<td>RxCpaAcrInterim</td>
<td>422</td>
</tr>
<tr>
<td>RxCpaAcrStart</td>
<td>422</td>
</tr>
<tr>
<td>RxCpaAcrStop</td>
<td>423</td>
</tr>
<tr>
<td>RxCpaMsgProcessed</td>
<td>423</td>
</tr>
<tr>
<td>TxCpaAnswerMsgToDrl</td>
<td>423</td>
</tr>
<tr>
<td>TxCpaMsgCopyInd</td>
<td>424</td>
</tr>
<tr>
<td>TxCpaRequestMsgToDrl</td>
<td>424</td>
</tr>
<tr>
<td>TxCpaTraceInd</td>
<td>424</td>
</tr>
<tr>
<td>Charging Proxy Application (CPA) Session DB measurements</td>
<td>425</td>
</tr>
<tr>
<td>EvCpaNoSbrAccess</td>
<td>426</td>
</tr>
<tr>
<td>EvCpaSbrAvgRespTime</td>
<td>427</td>
</tr>
<tr>
<td>EvCpaSbrCreateSess</td>
<td>427</td>
</tr>
<tr>
<td>Event Code</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>EvCpaSbrDeleteSess</td>
<td>427</td>
</tr>
<tr>
<td>EvCpaSbrPeekRespTime</td>
<td>428</td>
</tr>
<tr>
<td>EvCpaSbrQryErr</td>
<td>428</td>
</tr>
<tr>
<td>EvCpaSbrQryMatch</td>
<td>428</td>
</tr>
<tr>
<td>EvCpaSbrQryNoMatch</td>
<td>429</td>
</tr>
<tr>
<td>EvCpaSbrResponseTime</td>
<td>429</td>
</tr>
<tr>
<td>EvCpaSbrUpdateSess</td>
<td>429</td>
</tr>
<tr>
<td>RxCpaUndeliveredMsg</td>
<td>430</td>
</tr>
<tr>
<td>TxCpaSbrQueryTot</td>
<td>430</td>
</tr>
<tr>
<td>Communication Agent (ComAgent)</td>
<td>431</td>
</tr>
<tr>
<td>Exception measurements</td>
<td></td>
</tr>
<tr>
<td>CADataFIFOQueueFul</td>
<td>435</td>
</tr>
<tr>
<td>CADSTxDscrdCong</td>
<td>436</td>
</tr>
<tr>
<td>CAHSTxDscrdIntErrSR</td>
<td>436</td>
</tr>
<tr>
<td>CAHSTxDscrdCongSR</td>
<td>437</td>
</tr>
<tr>
<td>CAHSTxDscrdIntErrSR</td>
<td>437</td>
</tr>
<tr>
<td>CAHSTxDscrdUnavailSR</td>
<td>438</td>
</tr>
<tr>
<td>CAHSTxDscrdUnknownSR</td>
<td>438</td>
</tr>
<tr>
<td>CAHSTxDscrdUnkwnRsrc</td>
<td>439</td>
</tr>
<tr>
<td>CAHSTxRsrc</td>
<td>439</td>
</tr>
<tr>
<td>CAMxFIFOQueueFul</td>
<td>439</td>
</tr>
<tr>
<td>CARsrcPoolFul</td>
<td>440</td>
</tr>
<tr>
<td>CARSTxDscrdCong</td>
<td>441</td>
</tr>
<tr>
<td>CARSTxDscrdInternalErr</td>
<td>441</td>
</tr>
<tr>
<td>CARSTxDscrdSvcUnavail</td>
<td>441</td>
</tr>
<tr>
<td>CARxDiscUnexpEvent</td>
<td>442</td>
</tr>
<tr>
<td>CARTxDscrdBundle</td>
<td>442</td>
</tr>
<tr>
<td>CARxDscrdConnUnavail</td>
<td>443</td>
</tr>
<tr>
<td>CARxDscrdDecodeFailed</td>
<td>443</td>
</tr>
<tr>
<td>CARxDscrdIncompat</td>
<td>444</td>
</tr>
<tr>
<td>CARxDscrdInternalErr</td>
<td>444</td>
</tr>
<tr>
<td>CARxDscrdLayerSendFail</td>
<td>444</td>
</tr>
<tr>
<td>CARxDscrdMsgLenErr</td>
<td>445</td>
</tr>
<tr>
<td>CARxDscrdUnkServer</td>
<td>445</td>
</tr>
<tr>
<td>CARxDscrdUnkStkLyr</td>
<td>446</td>
</tr>
<tr>
<td>CARxMsgUnknown</td>
<td>446</td>
</tr>
<tr>
<td>CAStackQueueFul</td>
<td>446</td>
</tr>
<tr>
<td>CATransDscrdInvCorrId</td>
<td>447</td>
</tr>
<tr>
<td>CATransDscrdStaleErrRsp</td>
<td>447</td>
</tr>
<tr>
<td>CATransEndAbnorm</td>
<td>448</td>
</tr>
<tr>
<td>CATransEndAbnormRateAvg</td>
<td>448</td>
</tr>
<tr>
<td>CATransEndAbnormRateMax</td>
<td>449</td>
</tr>
</tbody>
</table>
Communication Agent (ComAgent) Performance measurements

CAAvgDataFIFOQueueUtil ................................................................. 461
CAAvgMxFIFOQueueUtil ............................................................... 462
CAAvgQueueUtil ............................................................................. 462
CAAvgRsrcPoolUtil ........................................................................ 463
CAAvgRxStackEvents ................................................................. 463
CAAvgTxStackEvents ................................................................. 464
CADSTx ......................................................................................... 464
CAHSTxRsrc ................................................................................ 464
CAHSTxRsrcRateAvg ..................................................................... 465
CAHSTxRsrcRateMax ..................................................................... 465
CAPeakDataFIFOQueueUtil ............................................................ 465
CAPeakMxFIFOQueueUtil ............................................................... 466
CAPeakQueueUtil ........................................................................... 466
CAPeakRsrcPoolUtil ....................................................................... 467
CAPeakRxStackEvents ............................................................... 467
CAPeakTxStackEvents ............................................................... 468
CARSTx ......................................................................................... 468
CARx ......................................................................................... 468
CARxBundled ................................................................................ 469
CARxEventsBundled ..................................................................... 469
Computer Aided Policy Making (CAPM) measurements ........................................................... 476
    CAPM_Temp_Invoked........................................................................................................ 477
    CAPM_CondSet_True...................................................................................................... 477
    CAPM_Action_Set_Fails................................................................................................. 478
    CAPM_MsgCopyTriggered............................................................................................... 478
    CAPM_RxRejectWithErrorAnswer.................................................................................. 478
    CAPM_RxSilentDiscard................................................................................................. 479
Connection Congestion measurements..................................................................................... 479
    ConnOnsetCL1............................................................................................................... 480
    ConnOnsetCL2............................................................................................................... 481
    ConnOnsetCL3............................................................................................................... 481
    ConnOnsetCL4............................................................................................................... 482
    EvEmrCongestionOnset................................................................................................. 482
    EvRemoteBusyCongestion............................................................................................ 483
    EvSmoothedEmrAvg..................................................................................................... 483
    EvSmoothedEmrPeak................................................................................................... 484
    RxRejectedConnCongestion.......................................................................................... 484
    TmConnInCL1.............................................................................................................. 485
    TmConnInCL2.............................................................................................................. 485
    TmConnInCL3.............................................................................................................. 486
    TmConnInCL4.............................................................................................................. 487
Connection Exception measurements...................................................................................... 487
    EvConnCerValFail......................................................................................................... 489
    EvConnCexIpChkFail................................................................................................. 489
    EvConnCnxFail........................................................................................................... 490
EvConnDnsFail ................................................................. 490
EvConnFarEndClose ...................................................... 491
EvConnManClose .......................................................... 491
EvConnPeerNumIpFail .................................................. 491
EvConnRelease ............................................................. 492
EvSockInitFail .............................................................. 492
EvConnTransFail .......................................................... 492
RxConnDupPkts .............................................................. 493
RxConnDupTsns ............................................................. 493
RxConnGapAckBlocks .................................................. 493
RxConnGapAckBlocks .................................................. 494
TxConnRetransSegs ....................................................... 494
TxConnSendFail ........................................................... 495

Connection Performance measurements ........................................ 495
EvConnCnxSuccess ........................................................ 498
EvPerConnQueueCongestionChange ................................ 498
RxConnAvgMPS ............................................................ 499
RxConnMsgs ................................................................. 499
RxConnOctets ............................................................... 500
RxConnPeakMPS .......................................................... 500
RxConnRecvBufAvg ..................................................... 500
RxConnRecvBufPeak .................................................... 501
RxMsgRateAvg ............................................................. 501
RxMsgRatePeak ........................................................... 502
TmRxMPSDelay_MaxCapacity ....................................... 503
TmRxMPSDelay_SharedCapacity ..................................... 503
TXConnMsgs ............................................................... 504
TxConnOctets ............................................................... 504
TxConnSendBufAvg ..................................................... 505
TxConnSendBufPeak .................................................... 505
TxConnTotalDataChunks ............................................. 506
TxPerConnQueueAvg ..................................................... 506
TxPerConnQueuePeak ................................................... 507

Diameter Signaling Router (DSR) Application Exception measurements ........................................ 507
RxApplRequestNoRoutes .............................................. 508
RxApplUnavailable ....................................................... 509
RxApplUnavailableForAnswer ..................................... 510
RxApplUnavailableForRequest ..................................... 510
TxCpaFullDRLRequestReject ....................................... 511
TxCpaFullDRLAnswerDiscard ...................................... 512
TxFabrFullDRLRequestReject ....................................... 512
Diameter Signaling Router (DSR) Application Performance measurements

RxApplAnswerFwdSuccess ................................................................. 518
RxApplAnswerReceived ................................................................. 519
RxApplRequestFwdSuccess ............................................................. 519
RxApplRequestReceived ................................................................. 519
RxCpaAnswerMsgQueueAvg ............................................................ 520
RxCpaAnswerMsgQueuePeak .......................................................... 520
RxCpaAnswerProcessed ............................................................... 520
RxCpaEventMsgQueueAvg .............................................................. 521
RxCpaEventMsgQueuePeak ............................................................ 521
RxCpaMsgRateAvg ...................................................................... 522
RxCpaMsgRatePeak .................................................................... 522
RxCpaRequestMsgQueueAvg .......................................................... 523
RxCpaRequestMsgQueuePeak ........................................................ 523
RxCpaRequestProcessed ............................................................... 523
RxDmiwfRequestMsgQueuePeak .................................................... 523
RxDmiwfRequestMsgQueueAvg ....................................................... 524
RxDmiwfAnswerMsgQueuePeak ..................................................... 524
RxDmiwfAnswerMsgQueueAvg ....................................................... 524
TxDmiwfFullDRLRequestReject ....................................................... 525
TxDmiwfFullDRLAnswerDiscard ..................................................... 525
RxDmiwfMsgRatePeak ................................................................ 526
RxDmiwfMsgRateAvg ................................................................. 527
RxDmiwfRequestProcessed ........................................................... 527
RxDmiwfAnswerProcessed ........................................................... 527
RxFabrMsgRateAvg ................................................................. 528
RxFabrMsgRatePeak ................................................................ 528
RxFabrRequestMsgQueueAvg ....................................................... 529
RxFabrRequestMsgQueuePeak ....................................................... 529
RxFabrRequestProcessed ........................................................... 530
RxGlaMsgRateAvg ................................................................. 530
RxGlaMsgRatePeak ................................................................ 531
RxGlaRequestMsgQueueAvg ....................................................... 531
RxGlaRequestMsgQueuePeak ....................................................... 532
RxGlaRequestProcessed ........................................................... 532
RxRbarMsgRateAvg ................................................................. 533
RxRbarMsgRatePeak ................................................................ 533
<table>
<thead>
<tr>
<th>Measurement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRbarRequestMsgQueueAvg</td>
<td>534</td>
</tr>
<tr>
<td>RxRbarRequestMsgQueuePeak</td>
<td>534</td>
</tr>
<tr>
<td>RxRbarRequestProcessed</td>
<td>535</td>
</tr>
<tr>
<td>TxAppITransSuccess</td>
<td>535</td>
</tr>
<tr>
<td>Diameter Egress Transaction measurements</td>
<td>535</td>
</tr>
<tr>
<td>RxAnswerExpectedAll</td>
<td>536</td>
</tr>
<tr>
<td>RxAnswerMsgQueueFullDiscard</td>
<td>537</td>
</tr>
<tr>
<td>TxAnswerTimeout</td>
<td>537</td>
</tr>
<tr>
<td>TxConnAnswerMsgs</td>
<td>538</td>
</tr>
<tr>
<td>TxConnectionFailed</td>
<td>538</td>
</tr>
<tr>
<td>TxConnRequestMsgs</td>
<td>538</td>
</tr>
<tr>
<td>TxRequestSuccessAllConn</td>
<td>539</td>
</tr>
<tr>
<td>Diameter Exception measurements</td>
<td>539</td>
</tr>
<tr>
<td>EvAppIdListInconsistency</td>
<td>544</td>
</tr>
<tr>
<td>EvConnCeaIdValFail</td>
<td>544</td>
</tr>
<tr>
<td>EvConnCexTO</td>
<td>545</td>
</tr>
<tr>
<td>EvConnDpaTO</td>
<td>545</td>
</tr>
<tr>
<td>EvConnNoConnApps</td>
<td>546</td>
</tr>
<tr>
<td>EvConnPrvFail</td>
<td>546</td>
</tr>
<tr>
<td>EvConnRejected</td>
<td>547</td>
</tr>
<tr>
<td>EvConnRejInsufficientIngressMps</td>
<td>547</td>
</tr>
<tr>
<td>EvConnRejMaxCapacityExceeded</td>
<td>547</td>
</tr>
<tr>
<td>EvConnWdFail</td>
<td>548</td>
</tr>
<tr>
<td>EvConnWdSuspect</td>
<td>548</td>
</tr>
<tr>
<td>EvMpCerIDValFail</td>
<td>549</td>
</tr>
<tr>
<td>EvTransLifetimeExceededMp</td>
<td>549</td>
</tr>
<tr>
<td>RxAnswerMsgQueueFullDiscard</td>
<td>550</td>
</tr>
<tr>
<td>RxAnswerUnexpected</td>
<td>550</td>
</tr>
<tr>
<td>RxConnCeaError</td>
<td>550</td>
</tr>
<tr>
<td>RxConnFailMalfMsg</td>
<td>551</td>
</tr>
<tr>
<td>RxConnInvalidMsg</td>
<td>551</td>
</tr>
<tr>
<td>RxConnMpCongestionAnswerRsp</td>
<td>552</td>
</tr>
<tr>
<td>RxConnOversizedMsg</td>
<td>552</td>
</tr>
<tr>
<td>RxConnUnexpCex</td>
<td>553</td>
</tr>
<tr>
<td>RxConnUnexpDpx</td>
<td>553</td>
</tr>
<tr>
<td>RxConnUnexpDwx</td>
<td>554</td>
</tr>
<tr>
<td>RxDOCRejectConn</td>
<td>554</td>
</tr>
<tr>
<td>RxDOCRejectConn</td>
<td>555</td>
</tr>
<tr>
<td>RxDOCRejectMp</td>
<td>555</td>
</tr>
<tr>
<td>RxMpCongestionDiscardMp</td>
<td>556</td>
</tr>
<tr>
<td>RxMpCongestionRejectMp</td>
<td>557</td>
</tr>
</tbody>
</table>
RxMsgsOCGreenPri0DiscardMp
RxMsgsOCYellowPri0DiscardMp
RxMsgsOCGreenPri1DiscardMp
RxMsgsOCYellowPri1DiscardMp
RxMsgsOCGreenPri2DiscardMp
RxMsgsOCYellowPri2DiscardMp
RxPduPoolEmptyDiscard
RxRoutableRejectMsgsMp
TmConnDegraded
TmConnEnabledNotAvail
TxAllConnQueueFullDiscard
TxConnCeaError
TxConnUnavailDiscard
TxReqMsgApplMismatch
TxReqMsgPerConnPtrMax
TxRequestEgressLoop
TxTestMessageDiscard
Diameter Ingress Transaction Exception measurements
RxAnsFwdFailed
RxDecodeFailure
RxDiscardedMsgsPerConnControlsMp
RxMpCongestionDiscardConn
RxDOCDiscardMp
RxDOCRejectConn
RxMessageLooping
RxMpCongestionDiscardConn
RxNoRoutesFound
RxNoRulesFailure
RxPrtRuleRejection
RxRejectedAll
RxRejectedOther
RxRequestMsgQueueFullDiscard
RxRoutableDiscardedMsgsMp
RxTransactionTimeout
TxAllConnQueueFullRequestReject
TxLongTimeoutPtrListEmpty
TxPerConnQueueFullDiscard
TxPerConnQueueFullAnswerDiscard
TxPerConnQueueFullRequestDiscard
TxPtrListEmpty
TxRerouteQueueFullReject
TxSockFullDiscard ................................................................................................................. 583
Diameter Ingress Transaction Performance measurements ........................................................ 583
RxConnRequestMsgs .................................................................................................................. 584
TxAnswer1xxx ............................................................................................................................ 585
TxAnswer2xxx ............................................................................................................................ 585
TxAnswer3xxx ............................................................................................................................ 586
TxAnswer4xxx ............................................................................................................................ 586
TxAnswer5xxx ............................................................................................................................ 586
TxAnswerFailure ......................................................................................................................... 587
TxAnswerLocalNode .................................................................................................................. 587
TxAnswerOther .......................................................................................................................... 588
Diameter Performance measurements .......................................................................................... 588
EvConnPrvSuccess ...................................................................................................................... 593
EvPerConnPtrQueueAvg .............................................................................................................. 594
EvPerConnPtrQueuePeak ............................................................................................................ 594
RoutingMsgs .............................................................................................................................. 595
RxAcceptedRequestsMp ............................................................................................................. 595
RxAcceptedMsgsPerConnControlsMp ....................................................................................... 595
RxAnswerExpectedAll ................................................................................................................ 596
RxAnswerExpectedAllMp .......................................................................................................... 596
RxAnswerExpectedRoutedMp .................................................................................................... 597
RxAnswerMsgsMp ....................................................................................................................... 597
RxConnAnswerMsgs .................................................................................................................. 598
RxConnCea ................................................................................................................................. 598
RxConnCer ................................................................................................................................. 598
RxConnDpa ................................................................................................................................ 599
RxConnDpr ................................................................................................................................ 599
RxConnDwa ................................................................................................................................ 599
RxConnDwr ................................................................................................................................ 600
RxConnOtherNonRoutable ........................................................................................................... 600
RxConnRequestMsgs .................................................................................................................. 600
RxConnRoutableMsgs ............................................................................................................... 601
RxMaxMpsAcceptedMp ............................................................................................................... 601
RxMaxMpsAcceptedRequestsMp ............................................................................................... 601
RxMsgSize .................................................................................................................................. 602
RxMsgSizeAvg ............................................................................................................................ 602
RxMsgSizePeak ........................................................................................................................... 603
RxMsgsOCPri0Mp ....................................................................................................................... 603
RxMsgsOCGreenPri0Mp .............................................................................................................. 604
RxMsgsOCYellowPri0Mp ............................................................................................................. 604
RxMsgsOCPri1Mp ....................................................................................................................... 604
<table>
<thead>
<tr>
<th>Category</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxMsgsOCGreenPri1Mp</td>
<td>605</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri1Mp</td>
<td>605</td>
</tr>
<tr>
<td>RxMsgsOCPri2Mp</td>
<td>605</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri2Mp</td>
<td>606</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri2Mp</td>
<td>606</td>
</tr>
<tr>
<td>RxMsgsOCPri3Mp</td>
<td>606</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri3Mp</td>
<td>606</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri3Mp</td>
<td>606</td>
</tr>
<tr>
<td>RxMsgsOCPri0RatePeakMp</td>
<td>607</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri0RatePeakMp</td>
<td>607</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri0RatePeakMp</td>
<td>607</td>
</tr>
<tr>
<td>RxMsgsOCPri1RatePeakMp</td>
<td>608</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri1RatePeakMp</td>
<td>608</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri1RatePeakMp</td>
<td>608</td>
</tr>
<tr>
<td>RxMsgsOCPri2RatePeakMp</td>
<td>609</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri2RatePeakMp</td>
<td>609</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri2RatePeakMp</td>
<td>609</td>
</tr>
<tr>
<td>RxMsgsOCPri3RatePeakMp</td>
<td>610</td>
</tr>
<tr>
<td>RxOfferedMsgsMp</td>
<td>610</td>
</tr>
<tr>
<td>RxRequestMsgsMp</td>
<td>610</td>
</tr>
<tr>
<td>RxRequestNoErrors</td>
<td>611</td>
</tr>
<tr>
<td>RxRequestNoErrorsMp</td>
<td>611</td>
</tr>
<tr>
<td>RxRoutableAcceptedMsgsMp</td>
<td>611</td>
</tr>
<tr>
<td>RxRoutableMsgsMp</td>
<td>612</td>
</tr>
<tr>
<td>TmConnAvail</td>
<td>612</td>
</tr>
<tr>
<td>TmConnPrvRspAvg</td>
<td>613</td>
</tr>
<tr>
<td>TmResponseTimeDownstream</td>
<td>613</td>
</tr>
<tr>
<td>TmResponseTimeDownstreamMp</td>
<td>613</td>
</tr>
<tr>
<td>TmResponseTimeUpstream</td>
<td>614</td>
</tr>
<tr>
<td>TxAnswerMsgsMp</td>
<td>614</td>
</tr>
<tr>
<td>TxConnAnswerMsgs</td>
<td>615</td>
</tr>
<tr>
<td>TxConnCea</td>
<td>615</td>
</tr>
<tr>
<td>TxConnCer</td>
<td>615</td>
</tr>
<tr>
<td>TxConnDpa</td>
<td>616</td>
</tr>
<tr>
<td>TxConnDpr</td>
<td>616</td>
</tr>
<tr>
<td>TxConnDwa</td>
<td>616</td>
</tr>
<tr>
<td>TxConnDwr</td>
<td>617</td>
</tr>
<tr>
<td>TxConnRequestMsgs</td>
<td>617</td>
</tr>
<tr>
<td>TxMsgSize</td>
<td>617</td>
</tr>
<tr>
<td>TxMsgSizeAvg</td>
<td>618</td>
</tr>
<tr>
<td>TxMsgSizePeak</td>
<td>618</td>
</tr>
<tr>
<td>TxRequestMsgsMp</td>
<td>619</td>
</tr>
<tr>
<td>TxRequestSuccessAllMP</td>
<td>619</td>
</tr>
</tbody>
</table>
Diameter Rerouting measurements ........................ 619
  RxRerouteAnswerRsp ........................................ 620
  RxRerouteAnswerRspMp ....................................... 621
  TxRerouteAnswerResponse .................................... 621
  TxRerouteAnswerTimeout ..................................... 621
  TxRerouteAttempts ............................................. 622
  TxRerouteConnFailure ......................................... 622
  TxRerouteSuccessSent ......................................... 623

DM-IWF Exception measurements ........................................ 623
  TxDmiwfMtoDRoutingFail .................................. 624
  TxDmiwfDtoMRoutingFail .................................... 625
  EvDmiwfDtoMtimeout ......................................... 626
  EvDmiwfPtrPoolExceeded .................................... 626
  RxDmiwfSS7MPAnswerUnexpected ......................... 627
  EvMdlwfSvcCongest ........................................... 627
  EvMdlwfError .................................................... 627
  EvMdlwfConnExhausted ...................................... 628
  RxDiscOnError .................................................... 628
  EvDmlwfTxFwdFail ............................................. 628
  EvDmiwfMsgSizeExceeded .................................... 629

DM-IWF Performance measurements ...................................... 629
  RxDmiwfDtoMTransCnt ........................................ 630
  RxDmiwfDtoMTransRateAvg ................................. 631
  RxDmiwfDtoMTransRatePeak .................................. 631
  RxDmiwfMtoDTransCnt ......................................... 632
  RxDmiwfMtoDTransRateAvg .................................... 632
  RxDmiwfMtoDTransRatePeak .................................. 632
  RxDmiwfTransactionRspQueuePeak ......................... 633
  RxDmiwfTransactionRspQueueAvg ......................... 633
  EvDmiwfPtrPoolPeak ........................................... 633
  EvDmiwfPtrPoolAvg ............................................. 634
  RxDmiwfRequestMessage ..................................... 634
  RxDmiwfAnswerMessage ...................................... 634
  TxDmiwfRequestMessage ..................................... 635
  TxDmiwfAnswerMessage ...................................... 635
  RxDmiwfRequestMessageIwf .................................. 635
  RxDmiwfAnswerMessageIwf .................................. 635
  TxDmiwfRequestMessageIwf .................................. 636
  TxDmiwfAnswerMessageIwf .................................. 636

Egress Throttle Group Performance measurements .................. 637
  TxEtgMsgsLocal ............................................... 638
TxEtgMsgRatePeak ............................................................................................................. 638
TxEtgMsgRateAvg ............................................................................................................... 639
EvEtgRateCongestionOnset ............................................................................................... 639
EvEtgRateDiscardPri0 ........................................................................................................... 640
EvEtgRateDiscardPri1 ........................................................................................................... 640
EvEtgRateDiscardPri2 ........................................................................................................... 641
EvEtgPendingTransPeak ..................................................................................................... 642
EvEtgPendingTransAvg ....................................................................................................... 642
EvEtgPendingTransCongestionOnset .................................................................................. 642
EvEtgPendingTransDiscardPri0 ......................................................................................... 643
EvEtgPendingTransDiscardPri1 ......................................................................................... 644
EvEtgPendingTransDiscardPri2 ......................................................................................... 644
Full Address Based Resolution (FABR) Application Exception measurements ............... 645
RxFabrBlacklistedImsi ....................................................................................................... 647
RxFabrBlacklistedMsisdn ................................................................................................. 647
RxFabrDecodeFailureResol ............................................................................................... 647
RxFabrInvalidImsiMcc ....................................................................................................... 648
RxFabrResolFailAll ............................................................................................................. 648
RxFabrResolFailCmdcode ................................................................................................. 648
RxFabrResolFailDpCongested ......................................................................................... 649
RxFabrResolFailImpiMatch .............................................................................................. 649
RxFabrResolFailImpuMatch .............................................................................................. 650
RxFabrResolFailMsisdnMatch ............................................................................................ 650
RxFabrResolFailNoAddrAvps ............................................................................................ 650
RxFabrResolFailNoValidAddr .......................................................................................... 651
RxFabrSrvNotiDpComAgentErrors .................................................................................. 652
RxFabrUnkAppId .............................................................................................................. 652
TxFabrDbConFail ............................................................................................................... 652
TxFabrFwdFail .................................................................................................................. 653
Full Address Based Resolution (FABR) Application Performance measurements ............. 653
FabrAverageQueriesPerBundle ....................................................................................... 655
RxDpResponseTimeAvg ...................................................................................................... 655
RxFabrAvgMsgSize ............................................................................................................ 656
RxFabrBundledResponseEvents ....................................................................................... 656
RxFabrDpResponseMsgQueueAvg .................................................................................... 656
RxFabrDpResponseMsgQueuePeak .................................................................................... 657
RxFabrMsgs ....................................................................................................................... 657
RxFabrResolAll ................................................................................................................... 657
RxFabrResolAllMp ............................................................................................................ 658
RxFabrResolImpi ............................................................................................................... 658
<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxFabrResolImpu</td>
<td>658</td>
</tr>
<tr>
<td>RxFabrResollMsli</td>
<td>659</td>
</tr>
<tr>
<td>RxFabrResolMsisdn</td>
<td>659</td>
</tr>
<tr>
<td>RxFabrResolRateAvg</td>
<td>660</td>
</tr>
<tr>
<td>RxFabrResolRatePeak</td>
<td>660</td>
</tr>
<tr>
<td>RxFabSrsvNotiDpCongest</td>
<td>660</td>
</tr>
<tr>
<td>TxFabrAbandonRequest</td>
<td>661</td>
</tr>
<tr>
<td>TxFabrBundledQueryEvents</td>
<td>661</td>
</tr>
<tr>
<td>TxFabFwdDefaultDest</td>
<td>661</td>
</tr>
<tr>
<td>TxFabFwdNochange</td>
<td>662</td>
</tr>
<tr>
<td>TxFabFwdSuccess</td>
<td>662</td>
</tr>
<tr>
<td>TxFabrMsgAttempt</td>
<td>662</td>
</tr>
<tr>
<td>GLA Exception measurements</td>
<td>663</td>
</tr>
<tr>
<td>RxGlaDecodeFailures</td>
<td>663</td>
</tr>
<tr>
<td>RxGlaDatabaseFailures</td>
<td>664</td>
</tr>
<tr>
<td>RxGlaDatabaseTimeouts</td>
<td>664</td>
</tr>
<tr>
<td>GLA Performance measurements</td>
<td>665</td>
</tr>
<tr>
<td>TxGlaSuccessMsgs</td>
<td>665</td>
</tr>
<tr>
<td>RxGlaResponseMsgQueuePeak</td>
<td>665</td>
</tr>
<tr>
<td>RxGlaResponseMsgQueueAvg</td>
<td>666</td>
</tr>
<tr>
<td>TxGlaSuccessMsgRatePeak</td>
<td>666</td>
</tr>
<tr>
<td>TxGlaSuccessMsgRateAvg</td>
<td>667</td>
</tr>
<tr>
<td>RxGlaFailureMsgs</td>
<td>667</td>
</tr>
<tr>
<td>IDIH measurements</td>
<td>667</td>
</tr>
<tr>
<td>EvIdihNumTtrsSent</td>
<td>668</td>
</tr>
<tr>
<td>EvIdihNumTtrsDeliveryFailed</td>
<td>668</td>
</tr>
<tr>
<td>TmIdihTraceSuspendedTime</td>
<td>668</td>
</tr>
<tr>
<td>TmIdihTraceThrottlingTime</td>
<td>669</td>
</tr>
<tr>
<td>EvIdihThrottlingTtrsDiscarded</td>
<td>669</td>
</tr>
<tr>
<td>IP Front End (IPFE) Exception measurements</td>
<td>669</td>
</tr>
<tr>
<td>PcapDroppedPackets</td>
<td>670</td>
</tr>
<tr>
<td>ThrottledPackets</td>
<td>670</td>
</tr>
<tr>
<td>TsaUnexpectedSctp</td>
<td>671</td>
</tr>
<tr>
<td>TsaUnexpectedTcp</td>
<td>671</td>
</tr>
<tr>
<td>TxReject</td>
<td>671</td>
</tr>
<tr>
<td>TxRejectSctp</td>
<td>672</td>
</tr>
<tr>
<td>IP Front End (IPFE) Performance measurements</td>
<td>672</td>
</tr>
<tr>
<td>AsNewAssociations</td>
<td>673</td>
</tr>
<tr>
<td>AsNewAssociationsSctp</td>
<td>673</td>
</tr>
<tr>
<td>IpfeNewAssociations</td>
<td>674</td>
</tr>
<tr>
<td>IpfeNewAssociationsSctp</td>
<td>674</td>
</tr>
</tbody>
</table>
RxIpfeBytes.............................................................................................................................674
RxIpfeBytesSctp......................................................................................................................675
RxIpfePackets..........................................................................................................................675
RxTsaBytes..............................................................................................................................675
RxTsaBytesSctp.......................................................................................................................676
RxTsaPackets..........................................................................................................................676
RxTsaPacketsSctp...................................................................................................................676
TsaNewAssociations..............................................................................................................677
TsaNewAssociationsSctp......................................................................................................677
TxAsBytes................................................................................................................................677
TxAsBytesSctp........................................................................................................................678
TxAsPackets............................................................................................................................678
TxAsPacketsSctp....................................................................................................................678

MD-IWF Exception Measurements.................................................................................................679
TxMdIwfSs7TransmitFailure................................................................................................680
RxMdIwfOrphanMapResponse...........................................................................................680
EvMdIwfMapResponseTimeout..........................................................................................681
RxMdIwfDiamNon2xxxAnswer..........................................................................................681
RxMdIwfOrphanDiamAnswer............................................................................................682
EvMdIwfDiamAnswerTimeout............................................................................................682
RxMdIwfDiamAnswerUnexpectedDiamP.................................................................682
TxMdIwfFailComAgentEnqueue.........................................................................................683
RxMdIwfComAgentError.....................................................................................................683
RxMdIwfDiamPduPoolEmpty.............................................................................................684
EvMdIwfInterwrkFail...........................................................................................................684
EvMdIwfInterwrkFailAddrTrans.........................................................................................684
EvMdIwfInterwrkFailMsgTrans.........................................................................................685
TxMdIwfDiamEdlEncodeFailure.........................................................................................685
EvMdIwfInterwrkFailCongest.............................................................................................686
EvMdIwfInterwrkFailFarEndResponse...............................................................................686
EvMdIwfInterwrkFailDsrInitiated.......................................................................................687
EvMdIwfInterwrkFailSysError............................................................................................687
EvMdIwfInterwrkFailResExh...............................................................................................687
EvMdIwfTransRejectByDiamExtNode...............................................................................688

MD-IWF Performance measurements.........................................................................................688
RxMdIwfSS7Msg....................................................................................................................691
TxMdIwfSS7Msg....................................................................................................................691
RxMdIwfMapRequestMsg....................................................................................................691
TxMdIwfMapRequestMsg....................................................................................................692
RxMdIwfMapResponseMsg..................................................................................................692
TxMdIwfMapResponseMsg..................................................................................................692
MD-IWF SS7 Performance measurements .......................... 704
RxMdIwfMapRequestMsgByOpcode ........................................ 704
RxMdIwfMapResponseMsgByOpcode ........................................ 705
TxMdIwfMapRequestMsgByOpcode ........................................ 705
TxMdIwfMapResponseMsgByOpcode ........................................ 705

MD-IWF Diam Performance Measurements .......................... 706
RxMdIwfDiamRequestMsgByCommandCode .......................... 706
RxMdIwfDiamAnswerMsgByCommandCode .......................... 706
TxMdIwfDiamRequestMsgByCommandCode .......................... 707
TxMdIwfDiamAnswerMsgByCommandCode .......................... 707

Message Copy measurements ........................................... 708
DASCopyAnswerRx ................................................................. 709
DASCopyDiscarded .............................................................. 709
DASCopyFailureMCCSNotProvisioned ................................. 710
DASCopyFailureMPCong ................................................... 710
DASCopyFailurePeerApplIdUnsup ...................................... 711
DASCopyFailureSizeExceeded ........................................... 711
DASCopyFailureRLNotProv .............................................. 712
DASCopyRetransmits ....................................................... 712
DASCopyRetransmitsExceeded ........................................ 713
DASCopyTx ................................................................. 713
DASCopyValidAnswer ..................................................... 713
TxMsgCopyQueueAve .......................................................... 714
TxMsgCopyQueueFullDiscard ........................................... 714
TxMsgCopyQueuePeak ..................................................... 715
Message Priority measurements ........................................ 715
ExConnPeerUnsupMp .......................................................... 716
ExConnUnexpMp ............................................................... 717
RxMsgPri0ApplRule .......................................................... 718
RxMpMsgPri0 ................................................................. 718
RxMsgPri0PeerRule .......................................................... 719
RxMsgPri1ApplRule .......................................................... 719
RxMpMsgPri1 ................................................................. 719
RxMsgPri1PeerRule .......................................................... 720
RxMsgPri2ApplRule .......................................................... 720
RxMpMsgPri2 ................................................................. 720
RxMsgPri2PeerRule .......................................................... 721
Message Processor (MP) Performance measurements ........ 721
EvDiameterProcessAvg .................................................... 725
EvDiameterProcessPeak .................................................. 725
EvLongTimeoutPtrPoolAvg ............................................... 726
EvLongTimeoutPtrPoolPeak ............................................. 726
EvMpCongestionEntered .................................................. 727
EvMpCongestionLevel1Entered ........................................ 727
EvMpCongestionLevel2Entered ....................................... 728
EvMpCongestionLevel3Entered ....................................... 728
EvMpDangerOfCongestionEntered ................................... 729
EvPduPoolAvg .............................................................. 730
EvPduPoolPeak ............................................................. 730
EvPtrListAvg ............................................................... 731
EvPtrListPeak .............................................................. 731
EvStasisModeMaxConnsExceeded ................................. 732
EvStasisModeMpCongestion..............................................................733
RxAnswerMsgQueueAvg.................................................................733
RxAnswerMsgQueuePeak...............................................................733
RxMsgRateAvgMp...........................................................................734
RxMsgRatePeakMp.........................................................................734
RxRequestMsgQueueAvg.................................................................735
RxRequestMsgQueuePeak...............................................................735
TmAnswerTimeAvg........................................................................736
TmAnswerTimePeak.......................................................................737
TmMpCongestion...........................................................................737
TmMpCongestionLevel1.................................................................738
TmMpCongestionLevel2.................................................................739
TmMpCongestionLevel3.................................................................740
TmMpDangerOfCongestion............................................................740
TmRequestTimeAvg.......................................................................741
TmRequestTimePeak.....................................................................741
TxAllConnQueueAvg.....................................................................742
TxAllConnQueuePeak....................................................................742
TxRerouteQueueAvg.....................................................................743
TxRerouteQueuePeak....................................................................743
OAM.ALARM measurements.........................................................................744
OAM.PERF Measurements..................................................................745
OAM.SYSTEM measurements...........................................................746
P-DRA Diameter Usage measurements...............................................748
  PdraGxTopoHidingApplied............................................................750
  PdraGxpTopoHidingApplied..........................................................750
  PdraRxTopoHidingApplied............................................................751
  RxBindCapApn2PcrfPool.................................................................751
  RxBindCapPcrfPool2Prt.................................................................751
  RxBindCap2PcrfSubPool.................................................................752
  RxCcrInitNoImsiMsgs.................................................................752
  RxPdra5002FromPcrf.................................................................753
  RxPdra5002FromPolicyClient.......................................................753
  RxPdraAarMsgs........................................................................753
  RxPdraAsrMsgs........................................................................754
  RxPdraCcrInitMsgs.....................................................................754
  RxPdraCcrTerminateMsgs.............................................................754
  RxPdraCcrUpdateMsgs...............................................................755
  GxpBindingSuccess.....................................................................755
  RxPdraGxpCcrInitMsgs...............................................................756
  RxPdraGxpCcrUpdateMsgs............................................................756
RxPdraGxpCcrTerminateMsgs
RxPdraMsgRateAvg
RxPdraMsgRatePeak
RxPdraRarGxMsgs
RxPdraRarGxpMsgs
RxPdraRarRxMsgs
RxPdraStrMsgs
TxPdraGxRarQuery
TxPdraGxRarRelease
P-DRA Diameter Exception measurements
RxBindCapPcrfPoolNotMapped
RxBindCapUnknownApn
RxBindCapMissingApn
RxBindDepUnknownApn
RxBindDepMissingApn
RxBindCapUnknownPcrf
RxPdraRequestProtocolErr
RxStackEventDiscardedCaFailure
TxAaxMsgDiscardedDueToDrlQueueFull
TxAsxMsgDiscardedDueToDrlQueueFull
TxCcxCcxMsgDiscardedDueToDrlQueueFull
TxPdraAnswersGeneratedForDiameterErr
TxPdraAnswersGeneratedForPsbrErrResp
TxPdraAnswersGeneratedConfigErr
TxPdraErrAnsGeneratedCAFailure
TxGxpCcxMsgDiscardedDrlQueueFull
TxRaxMsgDiscardedDueToDrlQueueFull
TxStxMsgDiscardedDueToDrlQueueFull
P-DRA Congestion Exception measurements
RxAarMsgDiscardedDueToCongestion
RxAsrMsgDiscardedDueToCongestion
RxCcCxRarGxMsgsDiscardedDueToCongestion
RxGxpCrrMsgDiscardedDueToCongestion
RxRarMsgDiscardedDueToCongestion
RxStrMsgDiscardedDueToCongestion
pSBR Binding Performance measurements
PsbrNewBindingsCreated
PsbrUpdatedBindings
PsbrBindTermByAscSess
PsbrAltKeyCreated
PsbrAltKeyDel
PsbrMaxBindingAgeAtTerm ................................................................. 775
PsbrAvgBindingAgeAtTerm ............................................................... 776
PsbrAvgBindingDbRead ................................................................. 776
PsbrMaxBindingDbRead ................................................................. 776
PsbrAvgBindingDbWrite ............................................................... 777
PsbrMaxBindingDbWrite ............................................................... 777
PsbrEarlySlaveBindingsCreated ..................................................... 777
PsbrFinalBindingsFollowed ........................................................... 778
PsbrSlavePollingContinue .............................................................. 778
PsbrSlavePollingRouteToPcrf ......................................................... 779
PsbrLockCollisions ................................................................. 780
TmPsbrProcessingTime .............................................................. 780

pSBR Session Performance measurements .......................................... 780
PsbrSessionsCreated ............................................................... 781
PsbrSessionsRefresh ............................................................... 782
PsbrSessionsDeleted ................................................................. 782
PsbrAvgSessionAgeTermPerAPN .................................................... 782
PsbrMaxSessionAgeTermPerAPN ................................................... 783
PsbrAvgSessionDbRead ............................................................... 783
PsbrMaxSessionDbRead ............................................................... 783
PsbrAvgSessionDbWrite ............................................................. 784
PsbrMaxSessionDbWrite ............................................................. 784
PsbrPendingRarLockCollisions ....................................................... 784

pSBR Binding Exception measurements ........................................... 785
PsbrCreateBindDbErr ................................................................. 786
PsbrUpdateBindDbErr ................................................................. 786
PsbrRemoveBindDbErr ............................................................... 786
PsbrCreateAltKeyDbErr ............................................................. 787
PsbrRemoveAltKeyDbErr ............................................................ 787
PsbrFindBindDbErr ................................................................. 787
PsbrEarlyTooLongSrRemoved ....................................................... 788
PsbrSlavePollingFail ................................................................. 788
PsbrSuspectSrRemoved ............................................................... 789

pSBR Session Exception measurements .............................................. 789
PsbrCreateSessDbErr ................................................................. 790
PsbrRefreshSessDbErr ............................................................... 790
PsbrRemSessDbErr ................................................................. 790
PsbrFindSessDbErr ................................................................. 791
PsbrRemSessRarAttempts ........................................................... 791

pSBR Audit measurements ............................................................. 792
PsbrImsiAuditDbErr ................................................................. 793
<table>
<thead>
<tr>
<th>Measurement</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrMsisdnAuditDbErr</td>
<td>793</td>
</tr>
<tr>
<td>PsbrIpv4AuditDbErr</td>
<td>794</td>
</tr>
<tr>
<td>PsbrIpv6AuditDbErr</td>
<td>794</td>
</tr>
<tr>
<td>PsbrSessionRecsAudited</td>
<td>794</td>
</tr>
<tr>
<td>PsbrExpiredSessionsFound</td>
<td>795</td>
</tr>
<tr>
<td>PsbrImsiRecsAudited</td>
<td>795</td>
</tr>
<tr>
<td>PsbrStaleSessionRemoved</td>
<td>795</td>
</tr>
<tr>
<td>PsbrIpv4RecsAudited</td>
<td>796</td>
</tr>
<tr>
<td>PsbrIpv4RecsRemoved</td>
<td>796</td>
</tr>
<tr>
<td>PsbrIpv6RecsAudited</td>
<td>796</td>
</tr>
<tr>
<td>PsbrSessionAuditDbErr</td>
<td>797</td>
</tr>
<tr>
<td>PsbrSessionRefAuditDbErr</td>
<td>797</td>
</tr>
<tr>
<td>PsbrImsiAuditCaErr</td>
<td>797</td>
</tr>
<tr>
<td>PsbrMsisdnAuditCaErr</td>
<td>797</td>
</tr>
<tr>
<td>PsbrIpv4AuditCongErr</td>
<td>798</td>
</tr>
<tr>
<td>PsbrIpv6AuditCongErr</td>
<td>798</td>
</tr>
<tr>
<td>PsbrIpv6RecsRemoved</td>
<td>799</td>
</tr>
<tr>
<td>PsbrMsisdnRecsAudited</td>
<td>799</td>
</tr>
<tr>
<td>PsbrMsisdnRecsRemoved</td>
<td>800</td>
</tr>
<tr>
<td>PsbrImsiRecsRemoved</td>
<td>800</td>
</tr>
<tr>
<td>PsbrImsiSrRemovedByAudit</td>
<td>801</td>
</tr>
<tr>
<td>PsbrMsisdnSrRemovedByAudit</td>
<td>801</td>
</tr>
<tr>
<td><strong>Peer Node Performance measurements</strong></td>
<td>802</td>
</tr>
<tr>
<td>RxPeerAnswers</td>
<td>802</td>
</tr>
<tr>
<td>RxPeerRequests</td>
<td>802</td>
</tr>
<tr>
<td>TxPeerAnswers</td>
<td>803</td>
</tr>
<tr>
<td>TxPeerRequests</td>
<td>803</td>
</tr>
<tr>
<td><strong>Peer Routing Rules measurements</strong></td>
<td>803</td>
</tr>
<tr>
<td>RxPrtSelected</td>
<td>804</td>
</tr>
<tr>
<td>RxRuleDuplicatePriority</td>
<td>805</td>
</tr>
<tr>
<td>RxRuleFwdFailActionSendAns</td>
<td>805</td>
</tr>
<tr>
<td>RxRuleFwdFailAll</td>
<td>806</td>
</tr>
<tr>
<td>RxRuleSelected</td>
<td>806</td>
</tr>
<tr>
<td>TxMsgPrtMarkedForCpy</td>
<td>807</td>
</tr>
<tr>
<td><strong>Route List measurements</strong></td>
<td>807</td>
</tr>
<tr>
<td>RxRouteListFailure</td>
<td>808</td>
</tr>
<tr>
<td>RxRouteListSelected</td>
<td>808</td>
</tr>
<tr>
<td>RxRouteListUnavailable</td>
<td>809</td>
</tr>
<tr>
<td>TmRouteListOutage</td>
<td>809</td>
</tr>
<tr>
<td><strong>Routing Usage measurements</strong></td>
<td>810</td>
</tr>
<tr>
<td>RxRoutedIntraMPAttempt</td>
<td>810</td>
</tr>
</tbody>
</table>
Session Binding Repository (SBR) Performance measurements

Sbr.TxShedCreatesTot
Sbr.TxShedWritesTot
Sbr.TxShedReadsTot
Sbr.TxShedAllTot

Sbr.RxCreate
Sbr.RxUpdate
Sbr.RxRead
Sbr.RxDelete
Sbr.RxStatus
Sbr.TxSuccess
Sbr.RxReqRatePeak
Sbr.RxServTimeAvg
Sbr.RxServTimePeak
Sbr.EvStaleRecRemoved
Sbr.EvCreateUpdateMod
Sbr.EvAvgSessionAge
Sbr.RxReqRateAvg
Sbr.EvSchdStaleRec
Sbr.EvStaleRecRevived
Sbr.EvMostlyStaleSessPartition
Sbr.EvAvgSessionAgePartition
Sbr.RxIngressMsgQueuePeak
Sbr.RxIngressMsgQueueAvg

SS7/Sigtran Measurements

Association Exception measurements
Association Performance measurements
Association Usage measurements
Link Exception measurements
Link Performance measurements
Link Set Performance measurements
Link Set Usage measurements
Link Usage measurements
Server M3UA Exception measurements
Server M3UA Performance measurements
Server M3UA Usage measurements
Server MTP3 Exception measurements
Server MTP3 Performance measurements
Server Resource Usage measurements
Server SCCP Exception measurements
Server SCCP Performance measurements
Appendix A: Policy DRA Error Resolution Procedures..............960

Error Code 500......................................................................................................................961
Error Code 501......................................................................................................................961
Error Code 502......................................................................................................................962
Error Code 2xx/3xx................................................................................................................963
Error Code 510......................................................................................................................963
Error Code 511......................................................................................................................964
Error Code 512......................................................................................................................964
Error Code 513......................................................................................................................965
Error Code 503......................................................................................................................966
Error Code 505......................................................................................................................967
Error Code 507......................................................................................................................968
Error Code 508......................................................................................................................968
Error Code 520......................................................................................................................969
Error Code 521......................................................................................................................969
Error Code 504......................................................................................................................970
Error Code 509......................................................................................................................971
Error Code 305......................................................................................................................971
Error Code 305......................................................................................................................972
Error Code 522......................................................................................................................972
Error Code 523......................................................................................................................973
Error Code 525......................................................................................................................973
Error Code 506......................................................................................................................974
Error Code 530......................................................................................................................975
Error Code 531......................................................................................................................975

Glossary................................................................................................................................977
List of Figures

Figure 1: Flow of Alarms.................................................................................................................................72
Figure 2: Alarm Indicators Legend..................................................................................................................72
Figure 3: Trap Count Indicator Legend........................................................................................................73
Figure 4: Breaker Panel LEDs.......................................................................................................................309
Figure 5: Breaker Panel Setting.....................................................................................................................310
List of Tables

Table 1: Admonishments................................................................................................................................56
Table 2: Data Export Elements.......................................................................................................................60
Table 3: Active Tasks Elements......................................................................................................................63
Table 4: Active Tasks Report Elements.........................................................................................................66
Table 5: Scheduled Tasks Elements..................................................................................................................67
Table 6: Alarm/Event ID Ranges ...................................................................................................................73
Table 7: Alarm and Event Types ...................................................................................................................74
Table 8: Schedule Active Alarm Data Export Elements .............................................................................76
Table 9: Schedule Event Data Export Elements...........................................................................................79
Table 10: Congestion Thresholds................................................................................................................107
Table 11: KPIs Server Elements....................................................................................................................360
Table 12: Schedule KPI Data Export Elements...........................................................................................361
Table 13: CAPM KPIs........................................................................................................................................363
Table 14: Charging Proxy Application (CPA) KPIs..................................................................................363
Table 15: Communication Agent KPIs........................................................................................................364
Table 16: Connection Maintenance KPIs...................................................................................................364
Table 17: DIAM KPIs......................................................................................................................................365
Table 18: DM-IWF KPIs................................................................................................................................365
Table 19: IPFE KPIs........................................................................................................................................366
Table 20: MP KPIs..........................................................................................................................................368
Table 21: FABR KPIs....................................................................................................................................368
Table 22: P-DRA KPIs....................................................................................................................................369
Table 73: P-DRA Congestion Exception Measurement Report Fields .................................................... 770
Table 74: pSBR Binding Performance Measurement Report Fields ...................................................... 772
Table 75: pSBR Session Performance Measurement Report Fields ........................................................ 780
Table 76: pSBR Binding Exception Measurement Report Fields ............................................................ 785
Table 77: pSBR Session Exception Measurement Report Fields ............................................................ 789
Table 78: pSBR Audit Measurement Report Fields ............................................................................... 792
Table 79: Peer Routing Rules Measurement Report Fields ...................................................................... 802
Table 80: Peer Routing Rules Measurement Report Fields ...................................................................... 804
Table 81: Route List Measurement Report Fields .................................................................................... 807
Table 82: Routing Usage Measurement Report Fields ............................................................................. 810
Table 83: Server TCAP Exception Measurement Report Fields .............................................................. 813
Table 84: Server TCAP Performance Measurement Report Fields ........................................................ 821
Table 85: SBR Exception Measurement Report Fields ............................................................................ 824
Table 86: SBR Performance Measurement Report Fields .......................................................................... 830
Table 87: Association Exception Measurement Report Fields .................................................................... 838
Table 88: Association Performance Measurement Report Fields ........................................................... 847
Table 89: Association Usage Measurement Report Fields .......................................................................... 849
Table 90: Link Exception Measurement Report Fields ............................................................................... 851
Table 91: Link Performance Measurement Report Fields ........................................................................... 854
Table 92: Link Set Performance Measurement Report Fields ...................................................................... 856
Table 93: Link Set Usage Measurement Report Fields ............................................................................... 858
Table 94: Link Usage Measurement Report Fields ..................................................................................... 859
Table 95: Server M3UA Exception Measurement Report Fields .......................................................... 862
Table 96: Server M3UA Performance Measurement Report Fields ....................................................... 866
Table 97: Server M3UA Usage Measurement Report Fields ..................................................................... 872
Table 98: Server MTP3 Exception Measurement Report Fields ..............................................................876
Table 99: Server MTP3 Performance Measurement Report Fields ..........................................................880
Table 100: Server Resource Usage Measurement Report Fields ..........................................................884
Table 101: Server SCCP Exception Measurement Report Fields ............................................................889
Table 102: Server SCCP Performance Measurement Report Fields .......................................................903
Table 103: SS7 Exception Measurement Report Fields .............................................................................911
Table 104: SS7 Performance Measurement Report Fields ........................................................................913
Table 105: Measurement Summary .............................................................................................................913
Table 106: RxTrFarEndClose ..........................................................................................................................917
Table 107: EvTrManClose ............................................................................................................................918
Table 108: EvTrNoRespClose ......................................................................................................................919
Table 109: EvTrCnxSuccess ..........................................................................................................................920
Table 110: EvTrCnxFail ................................................................................................................................921
Table 111: TxTrSendFail ...............................................................................................................................922
Table 112: RxTrRcvFailed .............................................................................................................................923
Table 113: EvTrSockInitFail .........................................................................................................................924
Table 114: TxTrOctets ...................................................................................................................................924
Table 115: RxTrOctets ...................................................................................................................................925
Table 116: TmTrEnaNotUp ..........................................................................................................................925
Table 117: RxTmSctpBufAvg .......................................................................................................................926
Table 118: RxTmSctpBufPeak ......................................................................................................................927
Table 119: TmSingleTransQueuePeak ........................................................................................................927
Table 120: TmSingleTransQueueAvg .........................................................................................................928
Table 121: TmSingleTransQueueFull .......................................................................................................929
Table 122: SctpTransPeerCWNDPeak ........................................................................................................930
Chapter 1

Introduction

Topics:
- Overview.....55
- Scope and Audience.....55
- Manual Organization.....55
- Documentation Admonishments.....56
- Related Publications.....56
- My Oracle Support (MOS).....56
- Emergency Response.....57
- Locate Product Documentation on the Oracle Technology Network Site.....57

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.
Overview

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

This documentation provides:

- 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 events history
- Information relevant to understanding KPIs in the application
- The procedure for viewing KPIs
- Lists of KPIs
- Information relevant to understanding measurements in the application
- Measurement report elements, and the procedures for printing and exporting measurements
- Lists of measurements by function

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, KPIs, and measurements 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 Technology Network Site.
- Alarms and Events, KPIs, and Measurements Overview provides general information about the application's alarms and events, KPIs, and measurements.
- 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.
- Measurements provides detailed measurement information, organized alphabetically by measurement category.
• *Policy DRA Error Resolution Procedures* provides information regarding various error codes associated with Policy DRA.

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Danger Icon](image) | Danger:  
(This icon and text indicate the possibility of *personal injury.*) |
| ![Warning Icon](image) | Warning:  
(This icon and text indicate the possibility of *equipment damage.*) |
| ![Caution Icon](image) | Caution:  
(This icon and text indicate the possibility of *service interruption.*) |
| ![Topple Icon](image) | Topple:  
(This icon and text indicate the possibility of *personal injury and equipment damage.*) |

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

My Oracle Support (MOS)

MOS ([https://support.oracle.com](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](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 **2** for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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](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.

---

**Locate Product Documentation on the Oracle Technology Network Site**

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) site, [http://docs.oracle.com](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 [www.adobe.com](http://www.adobe.com).

1. Log into the Oracle Technology Network site at [http://docs.oracle.com](http://docs.oracle.com).
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As.**
Chapter 2

Alarms and Events, KPIs, and Measurements Overview

Topics:

- Alarms Warning.....60
- Displaying the file list.....60
- Data Export.....60
- Tasks.....63

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

Displaying 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.
   
The Status & Manage Files page appears.

2. Select a server.
   All files stored on the selected server are displayed.

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
- Exporting measurements reports

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 Data Export page.

Table 2: Data Export Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Name of export server.</td>
<td>Must be a valid hostname, IPv4 address, or IPv6 address. Range: Maximum length is 24 characters; alphanumeric characters (a-z, A-Z, and 0-9) and</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
<td>Data Input Notes</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>minus sign. Hostname must start and end with an alphanumeric. To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Username used to access the export server</td>
<td>Format: Textbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: Maximum length is 32 characters; alphanumeric characters (a-z, A-Z, and 0-9). To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None</td>
</tr>
<tr>
<td>Directory on Export Server</td>
<td>Directory path on the export server where the exported data files are to be transferred</td>
<td>Format: Textbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: Maximum length is 255 characters; valid value is any UNIX string. Default: None</td>
</tr>
<tr>
<td>Path to rsync on Export Server</td>
<td>Optional path to the rsync binary on the export server</td>
<td>Format: Textbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: Maximum length is 4096 characters; alphanumeric characters (a-z, A-Z, and 0-9), dash, underscore, period, and forward slash. Default: If no path is specified, the username’s home directory on the export server is used</td>
</tr>
<tr>
<td>Backup File Copy Enabled</td>
<td>Enables or disables the transfer of the backup files.</td>
<td>Format: Checkbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Disabled (unchecked)</td>
</tr>
<tr>
<td>File Compression</td>
<td>Compression algorithm used when exported data files are initially created on the local host.</td>
<td>Format: Radio button</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: gzip, bzip2, or none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: gzip</td>
</tr>
<tr>
<td>Upload Frequency</td>
<td>Frequency at which the export occurs</td>
<td>Format: Radio button</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: fifteen minutes, hourly, daily or weekly</td>
</tr>
</tbody>
</table>
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. The Data Export page appears.
2. Enter a Hostname. See the 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. Enter the Path to Rsync on the Export server.
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. Click **Exchange SSH Key** to transfer the SSH keys to the export server. A password dialog box appears.

13. Enter the password. The server will attempt to exchange keys with the specified export server. After the SSH keys are successfully exchanged, continue with the next step.

14. Click **OK** or **Apply**. The export server is now configured and available to receive performance and configuration data.

**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 3: Active Tasks Elements**

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

Use this procedure to delete one or more tasks.

1. Select Status & Manage > Tasks > Active Tasks.
   
   The Active Tasks page appears.
   
   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.
   
   A confirmation box appears.

   5. Click OK to delete the selected task(s).
   
   The selected task(s) are deleted from the table.

Deleting all completed tasks

Use this procedure to delete all completed tasks.

1. Select Status & Manage > Tasks > Active Tasks.
   
   The Active Tasks page appears.
   
   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.

   A confirmation box appears.

   4. Click OK to delete all completed tasks.
   
   All tasks with the status of completed are deleted.

Canceling a running or paused task

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

1. Select Status & Manage > Tasks > Active Tasks.
   
   The Active Tasks page appears.
   
   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**.
   A confirmation box appears.
5. Click **OK** to cancel the selected task.
   The selected task is canceled.

**Pausing a task**

Use this procedure to pause a task.

1. Select **Status & Manage > Tasks > Active Tasks**.
   The **Active Tasks** page appears.
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.
   The selected task is paused. 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**.
   The **Active Tasks** page appears.
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 4: Active Tasks Report Elements

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

Generating an active task report

Use this procedure to generate an active task report.

1. Select **Status & Manage > Tasks > Active Tasks**.
   The **Active Tasks** page appears.

2. Select a server.
   
   **Note**: Hovering the mouse over any tab displays the name of the server.

3. Select one or more tasks.
   
   **Note**: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

4. Click **Report**.
   The **Tasks Report** page appears.

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**
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 5: Scheduled Tasks Elements

<table>
<thead>
<tr>
<th>Scheduled Tasks Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>Name given at the time of task creation</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the task</td>
</tr>
<tr>
<td>Time of Day</td>
<td>The hour and minute the task is scheduled to run</td>
</tr>
<tr>
<td>Day-of-Week</td>
<td>Day of the week the task is scheduled to run</td>
</tr>
<tr>
<td>Network Elem</td>
<td>The Network Element associated with the task</td>
</tr>
</tbody>
</table>

Editing a scheduled task

Use this procedure to edit a scheduled task.

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

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

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

2. Select one or more tasks.
3. Click Delete.
   A confirmation box appears.
4. Click OK to delete the selected task(s).
   The selected task(s) are deleted from the table.

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

1. Select Status & Manage > Tasks > Scheduled Tasks.
   The Scheduled Tasks page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.
   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

3. Click Report.
   The Scheduled Tasks Report page appears.
4. Click Print to print the report.
5. Click Save to save the report.
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 Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the View History GUI menu option.

**Note:** Some of the alarms in this document are shared with other applications and may not appear in this particular product.
• MD-IWF (33050-33099).....341
• GLA (33100-33149).....353
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).

The following figure shows how Alarms and Events are organized in the application.
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.
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 **AlarmID** listed for each alarm falls into one of the following process classifications:

**Table 6: Alarm/Event ID Ranges**

<table>
<thead>
<tr>
<th>Application/Process Name</th>
<th>Alarm ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPFE</td>
<td>5000-5099</td>
</tr>
<tr>
<td>OAM</td>
<td>10000-10999</td>
</tr>
<tr>
<td>IDIH</td>
<td>11500-11549</td>
</tr>
<tr>
<td>SBR</td>
<td>12000-12999</td>
</tr>
<tr>
<td>ComAgent</td>
<td>19800-19909</td>
</tr>
<tr>
<td>DSR Diagnostics</td>
<td>19910-19999</td>
</tr>
<tr>
<td>Diameter</td>
<td>22000-22350, 22900-22999</td>
</tr>
<tr>
<td>RBAR</td>
<td>22400-22424</td>
</tr>
<tr>
<td>Generic Application</td>
<td>22500-22599</td>
</tr>
</tbody>
</table>
### Alarms 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 7: Alarm and Event Types

<table>
<thead>
<tr>
<th>Type Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPL</td>
<td>Application</td>
</tr>
<tr>
<td>CAF</td>
<td>Communication Agent (ComAgent)</td>
</tr>
<tr>
<td>CAPM</td>
<td>Computer-Aided Policy Making (Diameter Mediation)</td>
</tr>
<tr>
<td>CFG</td>
<td>Configuration</td>
</tr>
<tr>
<td>CHG</td>
<td>Charging</td>
</tr>
<tr>
<td>CNG</td>
<td>Congestion Control</td>
</tr>
<tr>
<td>COLL</td>
<td>Collection</td>
</tr>
<tr>
<td>CPA</td>
<td>Charging Proxy Application</td>
</tr>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>DIAM</td>
<td>Diameter</td>
</tr>
<tr>
<td>DISK</td>
<td>Disk</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>DPS</td>
<td>Data Processor Server</td>
</tr>
<tr>
<td>Type Name</td>
<td>Type</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>ERA</td>
<td>Event Responder Application</td>
</tr>
<tr>
<td>FABR</td>
<td>Full Address Based Resolution</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>IDIH</td>
<td>Integrated DIH</td>
</tr>
<tr>
<td>IF</td>
<td>Interface</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPFE</td>
<td>IP Front End</td>
</tr>
<tr>
<td>LOADGEN</td>
<td>Load Generator</td>
</tr>
<tr>
<td>LOG</td>
<td>Logging</td>
</tr>
<tr>
<td>MEAS</td>
<td>Measurements</td>
</tr>
<tr>
<td>MEM</td>
<td>Memory</td>
</tr>
<tr>
<td>NP</td>
<td>Number Portability</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, Administration &amp; Maintenance</td>
</tr>
<tr>
<td>PDRA</td>
<td>Policy DRA</td>
</tr>
<tr>
<td>pSBR</td>
<td>Policy SBR</td>
</tr>
<tr>
<td>PLAT</td>
<td>Platform</td>
</tr>
<tr>
<td>PROC</td>
<td>Process</td>
</tr>
<tr>
<td>PROV</td>
<td>Provisioning</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>RBAR</td>
<td>Range-Based Address Resolution</td>
</tr>
<tr>
<td>REPL</td>
<td>Replication</td>
</tr>
<tr>
<td>SBRA</td>
<td>Session Binding Repository Application</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SDS</td>
<td>Subscriber Database Server</td>
</tr>
<tr>
<td>SIGC</td>
<td>Signaling Compression</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol Interface</td>
</tr>
<tr>
<td>SL</td>
<td>Selective Logging</td>
</tr>
<tr>
<td>SS7</td>
<td>Signaling System 7</td>
</tr>
<tr>
<td>SSR</td>
<td>SIP Signaling Router</td>
</tr>
<tr>
<td>STK</td>
<td>EXG Stack</td>
</tr>
</tbody>
</table>
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 NOAMP or SOAM. Alarm collection is handled solely by NOAMP servers in systems that do not support SOAMs.

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.

   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 8: Schedule Active Alarm Data Export Elements**

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

   **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 Displaying 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_180827.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.
   The View Active page appears.

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 is generated. This 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 NOAMP or SOAM. Alarm collection is handled solely by NOAMP servers in systems that do not support SOAMs.

1. Select **Alarms & Events > View History**.
   The View History page appears.
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 9: Schedule Event Data Export Elements**

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

---

**Table:**

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

Generating a report of historical alarms and events

Use this procedure to generate a report.

1. Select Alarms & Events > View History.
   
   The View History page appears.

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 is generated. This 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.
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.

5000 - IPFE Process Failure

**Alarm Type:** IPFE

**Description:** An IPFE process has stopped.

**Severity:** Critical

**Instance:** IP address of the application server

**HA Score:** Normal

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

**OID:** ipfelpfeProcessFailureNotify

**Recovery:** Contact *My Oracle Support (MOS)* for assistance.

5001 - IPFE Backend Unavailable

**Alarm Type:** IPFE

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

**Severity:** Minor

**Instance:** IP address of the application server

**HA Score:** Degraded

**Auto Clear Seconds:** N/A

**OID:** ipfelpfeBackendUnavailableNotify

**Recovery:** If a heartbeat is received from the application server, this alarm will clear.

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.

5002 - IPFE address configuration error

**Alarm Type:** IPFE
Description: The IPFE is unable to synchronize state data with its peer. This alarm can be issued for multiple reasons, including missing or invalid configurations, inability to bind a socket to the given IP address, or incompatible versions of software. The instance column provides more details when this alarm is raised. This alarm is present when the IPFE is activated but not yet configured.

Severity: Critical

Instance: One of the following strings:

- "ipfe1 and ipfe2 address both empty" - incomplete configuration
- "ipfe1 and ipfe2 address identical" - one of the addresses is incorrect
- "IPs are both local" - the two addresses correspond to the same interface on the blade
- "ipfe1 bad address" - invalid address format
- "ipfe2 bad address" - invalid address format
- "bind error" - cannot bind a socket to this interface address
- "cannot open ipfe device /dev/recent" - xt_recent module in TPD is either missing or incorrect
- "peer software version incompatible" - peer IPFE is on a different version

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfelpfeStateSyncConfigErrorNotify

Recovery: If the IPFE is able to successfully synchronize data with its peer, this alarm will clear.

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, contact My Oracle Support (MOS) for assistance.

5003 - IPFE state sync run error

Alarm Type: IPFE

Description: The IPFE was unable to synchronize state data with its mate.

Severity: Critical

Instance: One of the following strings:

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

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfelpfeStateSyncRunErrorNotify

Recovery: If the IPFE is able to synchronize state data with its mate, this alarm will clear.

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:
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.

3. Diagnose any network fault between the two IPFEs.
4. For further assistance, contact [My Oracle Support (MOS)](https://support.oracle.com).  

### 5004 - IPFE IP tables configuration error

**Alarm Type:** IPFE

**Description:** A target set address is configured with no IP addresses, or with invalid IP addresses. 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.

**Severity:** Critical

**Instance:** “tsa N address misconfiguration” where N is 1-16

**HA Score:** Normal

**Auto Clear Seconds:** N/A

**OID:** ipfIpfeIpTablesConfigErrorNotify

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

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

**Alarm Type:** IPFE

**Description:** 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:

- The application server has reached its maximum number of active Diameter connections
- The application server is congested. The application server will raise 22200 - [Local MP Congestion](https://support.oracle.com) also.
Severity: Minor

Instance: IP address of the application server in stasis

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfelpfeBackendInStasisNotify

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 Type: IPFE

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

Severity: Critical

Instance: "pcap <ethernet device name>"

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfelpfeEtherDeviceReadErrorNotify

Recovery: If the IPFE is able to read from the ethernet device, this alarm will clear.

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 Type: 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: ipfelpfeBackendUnderloadedNotify
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 Type: IPFE
Description: Traffic statistics reveal that an application server is processing higher than average load and will not receive new connections.
Severity: Minor
Instance: IP address of the overloaded application server
HA Score: Normal
Auto Clear Seconds: N/A
OID: ipfelpfeBackendOverloadedNotify
Recovery: When traffic statistics indicate that the application server is no longer overloaded, this alarm will clear.

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.
2. Check the status of the application servers by navigating to the Status & Manage > Server page.
3. Consult the application server's documentation for recovery steps.

5009 - No available servers in target set

Alarm Type: IPFE
Description: 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. 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.
Severity: Critical
Instance: "tsa N has no available servers" where N is 1-16
HA Score: Normal
Auto Clear Seconds: N/A
OID: ipfelpfeNoAvailableAppServersNotify
Recovery: When at least one application server in a target set becomes available, this alarm will clear.

1. Ensure that application servers have been configured for the target set address by viewing IPFE > Configuration > Target Sets.
2. Check the status of the application servers by navigating to the Status & Manage > Server page.
3. Consult the application server's documentation for recovery steps.
4. 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, contact *My Oracle Support (MOS)* for assistance.

### 5010 - Unknown Linux iptables command error

**Alarm Type:** IPFE

**Description:** The IPFE received an unknown error parsing Linux iptables output. This is an internal software error.

**Severity:** Critical

**Instance:** "error parsing iptables output"

**HA Score:** Normal

**Auto Clear Seconds:** N/A

**OID:** ipfeIpfeErrorParsingIptablesOutputNotify

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance.

### 5011 - System or platform error prohibiting operation

**Alarm Type:** IPFE

**Description:** The IPFE is unable to use its ethernet interfaces. This alarm is raised during the following conditions:

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

**Severity:** Critical

**Instance:**

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

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

**HA Score:** Normal

**Auto Clear Seconds:** N/A

**OID:** ipfelpfeSystemErrorNotify

**Recovery:** If the IPFE is able to use its ethernet interfaces, this alarm will clear.

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:
   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.
   5. If the alarm still does not clear, check the Ethernet devices and CPUs.

2. Contact **My Oracle Support (MOS)** for assistance.

### 5012 - Signaling interface heartbeat timeout

**Alarm Type:** IPFE

**Description:** Heartbeats to monitor the liveness of a signaling interface have timed out.

**Severity:** Critical

**Instance:** The name of the Ethernet interface affected, eg. "bond0.5" etc.

**HA Score:** Degraded

**Auto Clear Seconds:** N/A

**OID:** ipfelpfeSignalingInterfaceNotify

**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, contact **My Oracle Support (MOS).**

### 5013 - Throttling traffic

**Alarm Type:** 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

Auto Clear Seconds: N/A

OID: ipfelpfeThrottlingTrafficNotify

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, contact My Oracle Support (MOS).

5100 - Traffic overload

Alarm Type: IPFE

Description: Total IPFE signaling traffic rate is approaching or exceeding its engineered capacity. The severity thresholds are the following:
- Minor: set at 1.92 Gb/second, clear at 1.72 Gb/second
- Major: set at 2.56 Gb/second, clear at 2.36 Gb/second
- Critical set at 3.20 Gb/second, clear at 3.00 Gb/second

Severity: Minor, Major, Critical

Instance: N/A

Auto Clear Seconds: N/A

OID: ipfelpfeTrafficOverloadNotify

Recovery: If the signaling traffic declines below the clear threshold, the alarm will clear.

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. Contact My Oracle Support (MOS) for assistance.

5101 - CPU Overload

Alarm Type: IPFE

Description: CPU utilization is approaching maximum levels.

Severity: Major

Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
5102 - Disk Becoming Full

Alarm Type: IPFE
Description: Disk space utilization is approaching maximum levels.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

Contact My Oracle Support (MOS) for assistance.

5103 - Memory Overload

Alarm Type: IPFE
Description: IPFE memory utilization is approaching maximum levels.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Alarm Type: DB
Description: 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: 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 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:
   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: 
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:
   Contact My Oracle Support (MOS).

10008 - Database provisioning manually disabled
   Alarm Type: 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 Type: 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, contact My Oracle Support (MOS).

10010 - Stateful db from mate not yet synchronized
   Alarm Type: HA
   Description: The stateful database is not synchronized with the mate database.
   Severity: Minor
   Instance: N/A
HA Score: Degraded
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7OAGTStDbNoSyncNotify
Recovery:
  If alarm persists for more than 30 seconds, contact My Oracle Support (MOS).

10011 - Cannot monitor table
   Alarm Type: OAM
   Description: Monitoring for table cannot be set up.
   Severity: Major
   Instance: N/A
   HA Score: Degraded
   Auto Clear Seconds: This alarm does not autoclear.
   OID: awpss7OAGTCantMonitorTableNotify
   Recovery:
     Contact My Oracle Support (MOS).

10012 - Table change responder failed
   Alarm Type: OAM
   Description: The responder for a monitored table failed to respond to a table change.
   Severity: Major
   Instance: N/A
   HA Score: Degraded
   Auto Clear Seconds: This alarm does not autoclear.
   OID: awpss7OAGTResponderFailedNotify
   Recovery:
     Contact My Oracle Support (MOS).

10013 - Application restart in progress
   Alarm Type: HA
   Description: An application restart is in progress.
   Severity: Minor
   Instance: N/A
Alarms and Events

HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7OAGTAppISWDisabledNotify
Recovery:
   If duration of alarm is greater than two seconds, contact My Oracle Support (MOS).

10020 - Backup failure
   Alarm Type: DB
   Description: Database backup failed.
   Severity: Minor
   Instance: N/A
   HA Score: Normal
   Auto Clear Seconds: This alarm does not autoclear.
   OID: awpss7ApwBackupFailureNotify
   Recovery:
      Alarm will clear if a backup (Automated or Manual) of the same group data is successful. Contact My Oracle Support (MOS) if failures persist.

10050 - Resource Audit Failure
   Alarm Type: AUD
   Description: Database backup failed.
   Severity: Minor
   Instance:
   HA Score: Normal
   Auto Clear Seconds: 0
   OID: awpss7TekelecResourceAuditFailureNotify
   Recovery:

10051 - Route Deployment Failed
   Alarm Type: AUD
   Description: An error occurred in the deployment of a network.
   Severity: Minor
   Instance: Route ID that failed to deploy
   HA Score: Normal
Auto Clear Seconds: 0
OID: awpss7TekelecRouteDeploymentFailedNotify
Recovery:
   Edit the route to choose a gateway that is reachable or delete the route.

10052 - Route discovery failed
   Alarm Type: AUD
   Description: An error occurred in the discovery of network routes.
   Severity: Minor
   Instance: N/A
   HA Score: Normal
   Auto Clear Seconds: 0
   OID: awpss7TekelecRouteDiscoveryFailedNotify
   Recovery:
      If the problem persists, contact My Oracle Support (MOS).

10053 - Route deployment failed - no available device
   Alarm Type: AUD
   Description: A suitable device could not be identified for the deployment of a network route.
   Severity: Minor
   Instance: Route ID that failed to deploy
   HA Score: Normal
   Auto Clear Seconds: 0
   OID: awpss7TekelecNoRouteDeviceNotify
   Recovery:
      1. Deploy the route on a specific device instead of using the “AUTO” device.
      2. Ensure that every server in the server group has a usable device for the selected gateway.

10054 - Device deployment failed
   Alarm Type: AUD
   Description: An error occurred in the deployment of a network device.
   Severity: Minor
   Instance: Device name that failed to deploy
   HA Score: Normal
Auto Clear Seconds: 0
OID: awpss7TekelecDeviceDeploymentFailedNotify
Recovery:
   Edit or delete the device.

10055 - Device discovery failed

Alarm Type: AUD
Description: An error occurred in the discovery of network devices.
Severity: Minor
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: awpss7TekelecDeviceDiscoveryFailedNotify
Recovery:
   If the problem persists, contact My Oracle Support (MOS).

10073 - Server Group Max Allowed HA Role Warning

Alarm Type: HA
Description: The server group has received the maximum number of allowed HA role warnings
Severity: Minor
Instance: Affected Server Group name
HA Score: Normal
Auto Clear Seconds: 0
OID: 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

Alarm Type: HA

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

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: 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

Alarm Type: HA

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

Severity: Minor

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: 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

Event Type: HA

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

Severity: Info

Instance: N/A
HA Score: Normal
Throttle Seconds: 1
OID: awpss7FailureRecoveryWithoutAppRestartNotify
Recovery:
   Contact My Oracle Support (MOS).

10100 - Log export started
   Event Type: LOG
   Description: Log files export operation has started.
   Severity: Info
   Instance: N/A
   HA Score: Normal
   Throttle Seconds: 1
   OID: awpss7TekelecLogExportStartNotify
   Recovery:
      No action required.

10101 - Log export successful
   Event Type: LOG
   Description: The log files export operation completed successfully.
   Severity: Info
   Instance: N/A
   HA Score: Normal
   Throttle Seconds: 1
   OID: awpss7TekelecLogExportSuccessNotify
   Recovery:
      No action required.

10102 - Log export failed
   Event Type: LOG
   Description: The log files export operation failed.
   Severity: Info
   Instance: N/A
HA Score: Normal
Throttle Seconds: 1
OID: awpss7TekelecLogExportFailedNotify
Recovery:
1. Verify the export request and try the export again.
2. If the problem persists, contact My Oracle Support (MOS).

10103 - Log export already in progress
Event Type: LOG
Description: Log files export operation not run - export can only run on Active Network OAMP server.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 1
OID: awpss7TekelecLogExportNotRunNotify
Recovery:
   Restart export operation after existing export completes.

10104 - Log export file transfer failed
Event Type: LOG
Description: The performance data export remote copy operation failed.
Severity: Info
Instance: <Task ID>
Note: <Task ID> refers to the ID column found in Main Menu > Status & Manage > Tasks > Active Tasks.
HA Score: Normal
Throttle Seconds: 1
OID: awpss7TekelecExportXferFailedNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance.

10105 - Log export cancelled - user request
Event Type: LOG
Description: The log files export operation cancelled by user.
Severity: Info
Instance: <Task ID>
Note: <Task ID> refers to the ID column found in Main Menu > Status & Manage > Tasks > Active Tasks.
HA Score: Normal
Throttle Seconds: 1
OID: awpss7TekelecLogExportCancelledUserNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance.

10106 - Log export cancelled - duplicate request
Event Type: LOG
Description: The log files export operation was cancelled because a scheduled export is queued already.
Severity: Info
Instance: <Task ID>
Note: <Task ID> refers to the ID column found in Main Menu > Status & Manage > Tasks > Active Tasks.
HA Score: Normal
Throttle Seconds: 1
OID: 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, contact My Oracle Support (MOS) for assistance.

10107 - Log export cancelled - queue full
Event Type: LOG
Description: The log files export operation cancelled because the export queue is full.
Severity: Info
Instance: <Task ID>
Note: <Task ID> refers to the ID column found in Main Menu > Status & Manage > Tasks > Active Tasks.
HA Score: Normal
Throttle Seconds: 1
OID: awpss7TekelecLogExportCancelledQueueNotify
Recovery:
1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.

10108 - Duplicate scheduled log export task

Alarm Type: LOG
Description: A duplicate scheduled log export task has been queued.
Severity: Minor
Instance: <Target ID>

Note: <Target ID> refers to the scheduled task ID found by running a report from Main Menu > Status & Manage > Tasks > Scheduled Tasks.

HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7TekelecLogExportDupSchedTaskNotify

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, contact My Oracle Support (MOS) for assistance.

10109 - Log export queue is full

Alarm Type: LOG
Description: The log export queue is full
Severity: Minor
Instance: <Queue Name>

Note: <Queue Name> refers to the name of the queue used for the export task ID found by running a report from either 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, contact My Oracle Support (MOS) for assistance.
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
Instance: N/A
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: 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

Alarm Type: LOG

Description: SAML Login Successful
Severity: Info
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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

Alarm Type: LOG

Description: An attempt to login to the GUI via conventional login or via SSO login failed.
Severity: Info
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: awpss7TekelecSamlLoginFailedNotify

Recovery:

1. Use correct username and password to log in.
2. For failed SSO login, verify SSO was properly configured. Collect logs and contact My Oracle Support (MOS) if the problem persists.
10200 - Remote database reinitialization in progress

Alarm Type: CFG
Description: The remote database reinitialization is in progress. This alarm is raised on the active NOAMP server for the server being added to the server group.
Severity: Minor
Instance: <hostname of remote server>
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: 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, contact My Oracle Support (MOS).

IDIH (11500-11549)

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

11500 - Tracing Suspended

Alarm Group: IDIH
Description: IDIH trace has been suspended due to DA-MP (danger of) CPU congestion.
Severity: Minor
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterTracingSuspendedAlarmNotify
Recovery: No action required

11501 - Trace Throttling Active

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

**Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

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

**OID:** eagleXgDiameterTracingThrottledAlarmNotify

**Recovery:**

No action required

---

**11502 - Troubleshooting Trace Started**

**Event Group:** IDIH

**Description:** A troubleshooting trace instance was started.

**Severity:** Info

**Instance:** <TraceInstanceId>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterIDIHTraceStartedNotify

**Recovery:**

No action required.

---

**11503 - Troubleshooting Trace Stopped**

**Event Group:** IDIH

**Description:** A troubleshooting trace instance was stopped.

**Severity:** Info

**Instance:** <TraceInstanceId>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterIDIHTraceStoppedNotify

**Recovery:**

No action required.

---

**11504 - Invalid DIH IP Address**

**Alarm Group:** IDIH
**Description:** Unable to connect via ComAgent to remote DIH server with IP

**Severity:** Minor

**Instance:** String of Configured DIH IP Address

**HA Score:** Normal

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

**OID:** eagleXgDiameterInvalidDihIpAddressAlarmNotify

**Recovery:** No action required

---

**Session Binding Repository, SBR (12000-12010)**

This section provides information and recovery procedures for SBR alarms, which range from 12000 to 12999.

**12003 - SBR Congestion State**

**Alarm Type:** SBRA

**Description:** The SBR application is in a congested state and is shedding operations. The measurement Sbr.RxIngressMsgQueueAvg shows the average percentage of queue length utilization, which is used to determine congestion. The severity thresholds are the following:

**Table 10: Congestion Thresholds**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Set Threshold</th>
<th>Clear Threshold</th>
<th>Shed Operations</th>
<th>Associated Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor</td>
<td>60%</td>
<td>50%</td>
<td>Creates</td>
<td>Sbr.TxShedCreates</td>
</tr>
<tr>
<td>Major</td>
<td>80%</td>
<td>70%</td>
<td>Creates, Writes</td>
<td>Sbr.TxShedCreates, Sbr.TxShedWrites</td>
</tr>
<tr>
<td>Critical</td>
<td>95%</td>
<td>90%</td>
<td>Creates, Writes, Reads</td>
<td>Sbr.TxShedCreates, Sbr.TxShedWrites, Sbr.TxShedReads</td>
</tr>
</tbody>
</table>

**Severity:** Minor, Major, Critical

**Instance:** Sbr.RxIngressMsgQueueMetric[subId], SBR

**HA Score:** Normal

**Auto Clear Seconds:** N/A

**OID:** ipfeSbrCongestionStateNotify

**Recovery:** If congestion falls below the clear threshold, this alarm will clear.
The SBR congestion status exceeds the alarm threshold. Additional capacity may be required to service the traffic load. Contact My Oracle Support (MOS) for assistance.

12007 - SBR Active Sess Binding Threshold

**Alarm Type:** SBRA  
**Description:** The SBR application has exceeded its Active Session Binding threshold. The configuration, **Maximum active session bindings**, is used to calculate the percentage. The severity thresholds are the following:
- Minor: set at 70%, clear at 60%  
- Major: set at 80%, clear at 70%  
- Critical: set at 100%, clear at 90%

**Severity:** Minor, Major, Critical  
**Instance:** Sbr.EvCurrentSessionMetric, SBR  
**HA Score:** Normal  
**Auto Clear Seconds:** N/A  
**OID:** ipfeSbrActiveSessBindThresholdNotify  
**Recovery:** If total active session bindings fall below the clear threshold, this alarm will clear.

1. Select CPA > Configuration > SBR.  
The CPA > Configuration > SBR page appears.

2. Increase the **Maximum active session bindings** configuration if it is too low.

3. Click **Apply** to apply your changes.

Your changes will go into effect immediately.

4. The SBR active session bindings count exceeds the threshold. Additional capacity may be required to service the traffic load. Contact My Oracle Support (MOS) for assistance.

12010 - SBR Proc Term

**Alarm Type:** SBRA  
**Description:** The SBR application has terminated.

**Severity:** Critical  
**Instance:** sbr  
**HA Score:** Degraded  
**Auto Clear Seconds:** 10  
**OID:** ipfeSbrProcTermNotify  
**Recovery:** When an active SBR is terminated as indicated by this alarm, its standby becomes active. The Process Manager will automatically attempt to restart the terminated process. If the Process
Manager fails to start the terminated process, it will raise the alarm again. The standby that became active will remain active until it is placed into standby mode again.

1. Check the status of the terminated SBR by navigating to the Status & Manage > Server page.
2. If the Process Manager cannot restart the process, contact My Oracle Support (MOS) for assistance.

SS7/Sigtran Alarms (19200-19299)

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

19200 - RSP/Destination unavailable

Alarm Type: SS7
Description: Unable to access the SS7 Destination Point Code because the RSP status is Unavailable.
Severity: Critical
Instance: RSP Name
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7M3rlRspUnavailableNotify

Recovery:
1. RSP/Destination status can be monitored from the SOAM GUI 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, contact My Oracle Support (MOS).

19201 - RSP/Destination route unavailable

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

OID: awpss7M3rlRouteUnavailableNotify

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

19202 - Linkset unavailable

Alarm Type: SS7
Description: The SS7 link set to an adjacent signaling point has failed.
Severity: Major
Instance: <LinkSetName>
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7M3rlLinksetUnavailableNotify
Recovery:
1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link set status can be monitored from SS7/Sigtran > Maintenance > Linksets.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact My Oracle Support (MOS).

19203 - Link unavailable

Alarm Type: 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, contact My Oracle Support (MOS).

19204 - Preferred route unavailable

Alarm Type: 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, 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

Event Type: SS7

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

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7M3rlTfrReceivedNotify

Recovery:

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

19208 - TFC received

Event Type: SS7

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

Severity: Info

HA Score: Normal
Throttle Seconds: 30
Instance: N/A
OID: awpss7M3rlTfReceivedNotify
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 - invalid DPC

Event Type: SS7
Description: A message was discarded due to a routing error.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 10
OID: awpss7M3rlRoutingFailureNotify
Recovery:
1. Each MP’s assigned point code can be monitored from SS7/Sigtran > Configuration > Local Signaling Points.
2. If the event was caused by:
   • The DPC of an egress message is not configured as a remote signaling point, then look at the routing label in the event additional information, determine the DPC, and verify that the DPC is configured as an RSP.
   • The DPC of an egress message is configured but not available for routing, then look at the routing label in the event additional information, determine the DPC, verify that a route exists for the DPC, and use the RSP status screen to verify that a route is available for the RSP.
   • The DPC of an ingress message does not match the TPC or CPC of the MP server group, then either signaling is being misdirected by the STP toward the MP, or the MP server’s LSP is misconfigured. Look at the routing label in the event additional information for the OPC and DPC of the ingress message.
3. If a high number of these errors occurs, then an internal routing table problem may exist. Please contact My Oracle Support (MOS) for assistance.

19210 - M3RL routing error - invalid NI

Event Type: SS7
Description: The message was discarded due to a routing error. The NI (Network Indicator) value received in a message from the network is not assigned to the MP. This event is generated under the following circumstances:
- The NI in the MTP3 routing label of the ingress message is not supported for the given network signaling domain for a provisioned Local Signaling Point.
- For an ingress ANSI SCCP message, Bit-8 in the SCCP CDPA address indicator octet indicates that the CDPA is encoded as per international specifications:
  - A "0" in Bit 8 indicates that the address is international and that both the address indicator and the address are coded according to international specifications.
  - A "1" in Bit 8 indicates that the address is national and that both the address indicator and the address are coded according to national specifications.

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

**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** awpss7M3rlRoutingFailureInvalidNiNotify  
**Recovery:**
1. The Signaling Transfer Point or Signaling Gateway routing tables may be inconsistent with the NI assigned to the MP. You can monitor each MP’s assigned NI value from the GUI main menu under SS7/Sigtran > Configuration > Remote Signaling Points.
2. If the problem persists, 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, contact *My Oracle Support (MOS).*

**19217 - Node isolated - all links down**

**Alarm Type:** 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:** awpss7MrlnNodeIsolatedAllLinkDownNotify

**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, contact **My Oracle Support (MOS)**.

---

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

**Event Type:** SS7

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

**Severity:** Info

**Instance:** <AssocName>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** awpss7TimedOutWaitingForAspUpAckNotify

**Recovery:**

1. Verify 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, contact **My Oracle Support (MOS)**.

---

**19227 - Received unsolicited ASP-DOWN-ACK**

**Event Type:** SS7
**Description:** The adjacent server at the specified IP address and port has sent an ASP-DOWN-ACK, but not in response to an ASP-DOWN message from the MP server. Normally this indicates that the far-end of the association is being taken down for maintenance. If the association administrative state is **Enabled**, the MP server 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 **Blocked** or **Disabled**.

**Severity:** Info

**Instance:** <AssocName>

**HA Score:** Normal

**Throttle Seconds:** 30

**OID:** awpss7ReceivedUnsolicitedAspDownAckNotify

**Recovery:**
1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. If the problem persists, 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, 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: 10
OID: awpss7ReceivedUnsolicitedAspInactiveAckNotify
Recovery:
1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. If the problem persists, contact My Oracle Support (MOS).

19231 - Received invalid M3UA message

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

Recovery:
1. Examine the M3UA error code and the diagnostic information and attempt to determine why the
far-end of the link sent the malformed message.
   • Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
   • Error code 0x03 indicates an unsupported M3UA message class.
   • Error code 0x04 indicates an unsupported M3UA message type.
   • Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct
     parameter that does not belong in the message or occurs too many times in the message.
   • Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but
     value is out of range.
   • Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
   • Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter.
     The differences between this error and "Protocol Error" are subtle. Protocol Error is used when
     the parameter is recognized, but not intended for the type of message that contains it. Unexpected
     Parameter is used when the parameter identifier is not known.
   • Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing
     required conditional parameter.
   • Error code 0x19 indicates an invalid routing context. Received routing context not configured
     for any linkset using the association on which the message was received.

2. If the problem persists, contact My Oracle Support (MOS).
19233 - Failed to send non-DATA message

Event Type: SS7

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

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

Severity: Info

Instance: <LinkName> or <AssocName>

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

HA Score: Normal

Throttle Seconds: 10

OID: awpss7FailedToSentNonDataMessageNotify

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, 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, 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, contact [My Oracle Support (MOS)](https://support.oracle.com).
19240 - Remote SCCP subsystem prohibited

**Alarm Type:** SS7

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

**Severity:** Minor

**Instance:** <RMU>

**HA Score:** Normal

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

**OID:** awpss7RemoteSccpSubsystemProhibitedNotify

**Recovery:**

1. You can monitor destination status from **SS7/Sigtran > Maintenance > Remote Signaling Points** and RMU/subsystem status from **SS7/Sigtran > Maintenance > Remote MTP3 Users**.
   - If the subsystem’s status changed to **Prohibited** because SCMG received a SSP message, an audit of the status of the RMU via the SCCP subsystem status test (SST) procedure is performed.
   - If the subsystem’s status changed to **Prohibited** because SCCP received a MTP-PAUSE indication from M3RL, then recovery actions of restoring the RSP/Destination status to **Available** will be invoked by M3RL.
   - If the subsystem’s status changed to **Prohibited** because SCCP received a MTP STATUS cause=unequipped user indication from M3RL, then no automatic recovery will be initiated. Only manual action at the remote node can correct a remote point code that has not been configured with SCCP.
   - If the subsystem’s status changed to **Prohibited** because SCCP received a MTP STATUS cause=unknown or inaccessible indication from M3RL, then SCCP will automatically invoke subsystem status testing depending upon the network type:
     - ANSI: subsystem status testing of all RMUs associated with the point code.
     - ITU: subsystem status testing SCMG (**SSN=1**) associated with the point code.

2. Verify that IP network connectivity exists between the MP server and the adjacent servers.

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

4. Verify 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, contact **My Oracle Support (MOS)**.

19241 - SCCP message type unrecognizedSCCP malformed or unsupported message

**Event Type:** SS7

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

**Severity:** Info
19242 - SCCP Hop counter violation

Event Type: SS7
Description: SCCP discarded an ingress message because a Hop Counter violation was detected.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 30
OID: awpss7SccpHopCounterViolationNotify
Recovery:
1. One of the following conditions causes this error:
   • The originator of the message is setting the initial value too low.
   • The message is being rerouted too many times by the STPs, possibly because of an STP routing misconfiguration that has caused message looping.
2. Contact My Oracle Support (MOS).

19243 - SCCP routing failure

Event Type: SS7
Description: SCCP was unable to route or process a UDT or XUDT message during SCCP processing for reasons (other than a global title translation failure, detected SCCP loop) possibly requiring operator intervention.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 30
OID: awpss7SccpRoutingFailureNotify

Recovery:

1. These failures are typically associated with invalid information received in the SCCP messages. Check for the following:
   - A misconfiguration of the SCCP at the originating or terminating node
   - Network routing misconfiguration at the STPs
2. If the problem persists, contact My Oracle Support (MOS).

19244 - SCCP routing failure network status

Event Type: SS7

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

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpRoutingFailureNetworkStatusNotify

Recovery:

1. Typically these routing failures occur due to transient conditions such as RSP/Destination and Subsystem failures. Destination status can be monitored from the SOAM GUI SS7/Sigtran > Maintenance > Remote Signaling Points and RMU/Subsystem status can be monitored from SS7/Sigtran > Maintenance > Remote MTP3 Users.
2. 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.
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, contact My Oracle Support (MOS).

19245 - SCCP GTT failure

Event Type: SS7

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

Severity: Info

Instance: N/A
19246 - Local SCCP subsystem prohibited

**Alarm Type:** SS7

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

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

**Severity:** Major

**Instance:** <LSP>, <SSN>

**HA Score:** Normal

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

**OID:** awpss7SCCPLocalSubsystemProhibitedNotify

**Recovery:**

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

Event Type: SS7  
Description: SCCP Segmentation Procedure Failure  
Severity: Info  
Instance: N/A  
HA Score: Normal  
Throttle Seconds: 30  
OID: awpss7ScpSegmentationFailureNotify  
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. Contact the My Oracle Support (MOS) for assistance.

19249 - SCCP Reassembly Failure

Event Type: SS7  
Description: SCCP Segmentation Procedure Failure  
Severity: Info  
Instance: N/A  
HA Score: Normal  
Throttle Seconds: 30  
OID: awpss7ScpReassemblyFailureNotify  
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. Contact the My Oracle Support (MOS) for assistance.

19250 - SS7 process CPU utilization

Alarm Type: 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:** awpss7s7ProcessCpuUtilizationNotify

**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, contact **My Oracle Support (MOS)**.

---

**19251 - Ingress message rate**

**Alarm Type:** SS7

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

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

**Instance:** N/A

**HA Score:** Normal

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

**OID:** awpss7IngressMsgRateNotify

**Recovery:**
1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from 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, contact *My Oracle Support (MOS)*.

### 19252 - PDU buffer pool utilization

**Alarm Type:** SS7  
**Description:** The percent utilization of the MP’s PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded.  
**Severity:** Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active.  
**Instance:** <PoolName> Values: ANSI, ITUI, ITUN  
**HA Score:** Normal  
**Auto Clear Seconds:** This alarm does not autoclear.  
**OID:** awpss7PduBufferPoolUtilNotify

**Recovery:**

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from 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, contact *My Oracle Support (MOS)*.

### 19253 - SCCP stack event queue utilization

**Alarm Type:** SS7  
**Description:** The percent utilization of the MP’s SCCP stack event queue is approaching its maximum capacity.  
**Severity:** Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active.  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** This alarm does not autoclear.  
**OID:** awpss7SccpStackEventQueueUtilNotify

**Recovery:**
1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining
MPs in the server site. You can view MP server status from 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, contact My Oracle Support (MOS).

19254 - M3RL stack event queue utilization

Alarm Type: SS7
Description: The percent utilization of the MP’s M3RL Stack Event Queue is approaching its maximum
capacity.
Severity: Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active.
Instance: N/A
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7M3rlStackEventQueueUtilNotify

Recovery:
1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining
MPs in the server site. You can view MP server status from 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, contact My Oracle Support (MOS).

19255 - M3RL network management event queue utilization

Alarm Type: SS7
Description: The percent utilization of the MP's M3RL Network Management Event Queue is approaching its maximum capacity.

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

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlNetMgmtEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from 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, contact My Oracle Support (MOS).

19256 - M3UA stack event queue utilization

Alarm Type: 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, contact **My Oracle Support (MOS)**.

### 19258 - SCTP Aggregate Egress queue utilization

**Alarm Type:** SS7

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

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

**Instance:** N/A

**HA Score:** Normal

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

**OID:** awpss7SctpAggregateAssocWriteQueueUtilNotify

**Recovery:**

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.

2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events > View Active**.

3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from 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, contact **My Oracle Support (MOS)**.

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

**Event Type:** SS7

**Description:** Operation discarded due to local resource limitation

**Severity:** Info

**Instance:** Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapOpDiscardedLocalResLimitNotify
Recovery:
1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. 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

Event Type: SS7
Description: Transaction could not be delivered to remote TCAP peer due to conditions in the network.
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapTransNotDeliveredToPeerNotify
Recovery:
1. This event indicates that an SCCP service message (UDTS or XUDTS) was received from the network, meaning that the TCAP message could not be delivered to the remote TCAP peer. The event additional information field contains the first 80 octets of the SS7 message starting with the MTP3 routing label. This data can be used to determine the routing instructions for the message.
2. Verify that the routing is configured correctly for the destination. if the routing configuration is correct, determine why the remote TCAP peer is not available.
3. Contact My Oracle Support (MOS) for assistance if needed.

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

Event Type: SS7
Description: Operation discarded due to malformed component received from remote TCAP peer
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapMalformedComponentFromRemoteNotify
Recovery:
1. This event indicates that a TCAP component was received from the remote TCAP peer that could not be successfully decoded.
2. The event additional information field includes the reason why the decoding failed, plus the first 80 octets of the message starting with the MTP3 routing label. The message data can be used to determine the source of the malformed message.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

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

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

**Recovery:**
1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. Contact *My Oracle Support (MOS)* for assistance if needed.

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

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

**Recovery:**
1. This event indicates 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. Contact *My Oracle Support (MOS)* for assistance if needed.
19265 - Unexpected event received from local TC User

Event Type: SS7
Description: Unexpected event received from local TC User.
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapUnexpectedMsgFromLocalNotify

Recovery:
1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. The event additional information field includes a description of what event was received and why it was unexpected, as well as what was done with the operation or dialogue as a result.
3. Contact My Oracle Support (MOS) for assistance if needed.

19266 - Unexpected event received from remote TCAP peer

Event Type: SS7
Description: Unexpected event received from remote TCAP peer
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapUnexpectedMsgFromRemoteNotify

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

19267 - Dialogue removed by dialogue cleanup timer

Event Type: SS7
Description: Dialogue removed by dialogue cleanup timer
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapDialogueRemovedTimerExpiryNotify

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

19268 - Operation removed by invocation timer expiry

Event Type: SS7
Description: Operation removed by invocation timer expiry
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapOperationRemovedTimerExpiryNotify

Recovery:
1. This event indicates that a TCAP transaction containing no components was sent, but no response was received from the remote TCAP peer.
2. The event additional information field includes:
   - the local dialogue-id and invoke-id
   - the number of milliseconds that elapsed between the time the message was sent and the time that the operation was discarded
   - the destination point code to which the message was destined if the component was ever sent
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. Contact My Oracle Support (MOS) for assistance if needed.

---

### 19269 - Dialogue aborted by remote TCAP peer

**Event Type:** SS7  
**Description:** Dialogue aborted by remote TCAP peer  
**Severity:** Info  
**Instance:** Application name  
**HA Score:** Normal  
**Throttle Seconds:** 30  
**OID:** awpss7TcapDialogueAbortByRemoteNotify  
**Recovery:**

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

---

### 19270 - Received unsupported TCAP message

**Event Type:** SS7  
**Description:** Received unsupported TCAP message  
**Severity:** Info  
**Instance:** Application name  
**HA Score:** Normal  
**Throttle Seconds:** 30  
**OID:** awpss7TcapUnsupportedTCAPMsgRcvdNotify  
**Recovery:**
1. This event indicates that an unsupported TCAP message has been received.
2. The event additional information field includes:
   • the abort reason
   • the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the unsupported message.
4. Contact My Oracle Support (MOS) for assistance if needed.

19271 - Operation rejected by remote TCAP peer

Event Type: SS7
Description: Operation rejected by remote TCAP peer
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 30
OID: awpss7TcapReturnRejectByRemoteNotify
Recovery:
1. This event indicates that a remote TCAP peer has rejected an operation.
2. The event additional information field includes:
   • the reject reason
   • the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the message.
4. Contact My Oracle Support (MOS) for assistance if needed.

19272 - TCAP active dialogue utilization

Alarm Type: SS7
Description: TCAP active dialogue utilization
Severity: Minor, Major, Critical
Instance: Application name
HA Score: Normal
Auto Clear Seconds: 0 (alarm doesn’t auto-clear)
OID: awpss7TcapActiveDialogueUtilNotify
Recovery:
1. The percent utilization of the MP’s dialogue table is approaching maximum capacity. This alarm indicates that the number of active dialogues on the MP server is higher than expected.
2. If this problem persists and the dialogue table reaches 100% utilization, all new messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This condition may be caused by any of the following:

- the incoming plus outgoing rate of new dialogues is higher than expected (possibly due to poor load balancing across MP servers, or too few MP servers to handle the load)
- the duration of the dialogues is longer than expected
- both the rate and duration are higher than expected
- a software problem is preventing removal of completed dialogues

3. Contact My Oracle Support (MOS) for assistance if needed.

19273 - TCAP active operation utilization

**Alarm Type:** SS7  
**Description:** TCAP active operation utilization  
**Severity:** Minor, Major, Critical  
**Instance:** Application name  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (alarm doesn't auto-clear)  
**OID:** awpss7TcapActiveOperationUtilNotify

**Recovery:**

1. The percent utilization of the MP's component table is approaching maximum capacity. This alarm indicates that the number of active egress TCAP operations on the MP server is higher than expected.

2. If this problem persists and the component table reaches 100% utilization, all new egress operations will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This may be caused by any of the following:

- the outgoing rate of new operations is higher than expected (possibly due to a higher than expected average number of operations per message)
- the duration of the operations is longer than expected
- both the outgoing rate and duration are higher than expected
- a software problem is preventing removal of components

3. Contact My Oracle Support (MOS) for assistance if needed.

19274 - TCAP stack event queue utilization

**Alarm Type:** SS7  
**Description:** TCAP stack event queue utilization  
**Severity:** Minor, Major, Critical  
**Instance:** Application name  
**HA Score:** Normal
**Auto Clear Seconds**: 0 (alarm doesn’t auto-clear)

**OID**: awpss7TcapStackEventQueueUtilNotify

**Recovery**:

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

**19275 - Return error from remote TCAP peer**

**Event Type**: SS7

**Description**: Return error from remote TCAP peer

**Severity**: Info

**Instance**: Application name

**HA Score**: Normal

**Throttle Seconds**: 30

**OID**: awpss7TcapReturnErrorFromRemoteNotify

**Recovery**:

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

**19276 - SCCP Egress Message Rate**

**Alarm Type**: SS7

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

**Severity**: Major

**Instance**: Application name
HA Score: Normal
Auto Clear Seconds: 0 (alarm doesn't auto-clear)
OID: awpss7SccpEgressMsgRateNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance if needed.

19281 - TCAP Routing Failure

Event Type: SS7
Description: TCAP was unable to route message due to transient condition such as destination failure or destination unavailability
Severity: Info
Instance: Application name
HA Score: Normal
Throttle Seconds: 10
OID: awpss7TcapRoutingFailureNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance if needed.

Transport Manager Alarms and Events (19400-19499)

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

19400 - Transport Down

Alarm Type: TMF
Description: Transport Down
Severity: Major
Instance: <TransportName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: awptransmgrTransportDownNotify
Recovery:
   1. The Active alarm instance data, which can be viewed from 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, contact **My Oracle Support (MOS).**

### 19401 - Failed to configure Transport

**Event Type:** TMF

**Description:** Failed to configure Transport

**Severity:** Info

**Instance:** <TransportName>

**HA Score:** Normal
Throttle Seconds: 0 (zero)
OID: awptransmgrFailedToConfigureTransportNotify
Recovery:
1. A Transport is configured each time the Transport attempts to connect or reconnect.
2. If transport configuration fails or the alarm persists, contact *My Oracle Support (MOS)* for assistance.

19402 - Failed to connect Transport

Event Type: TMF
Description: Failed to connect Transport
Severity: Info
Instance: <TransportName>
HA Score: Normal
Throttle Seconds: 60
OID: awptransmgrFailedToConnectTransportNotify
Recovery:
1. The Transport named in the Instance field has failed in a connection attempt. If configured as an SCTP Initiator, the system will automatically attempt to recover the association/connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If configured as an SCTP or UDP Listener, no further action is taken.
   To troubleshoot
   • Verify that the transport’s local IP address and port number are configured on the Adjacent Node (Some Nodes will only accept connections from IP addresses and ports they are configured to accept connections from).
   • Verify that the transport’s remote IP address and port correctly identify an SCTP listening port on the adjacent node.
   • Verify that IP network connectivity exists between the MP and the adjacent node.
   • Verify that the timers in the transport’s configuration set are not set too short to allow the connection to proceed. This should be rare if the IP network is functioning correctly.
   • Check the event history logs at 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, contact *My Oracle Support (MOS).*

19403 - Received malformed SCTP message (invalid length)

Alarm Type: TMF
Description: Received malformed SCTP message (invalid length)
Severity: Info
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, 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, contact My Oracle Support (MOS).

19406 - Local Transport maintenance state change

Event Type: TMF
Description: Local Transport maintenance state change
Severity: Info
Instance: <TransportName>
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: awptransmgrLocalTransportMaintenanceStateChangeNotify

Recovery:

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

   Transport status can be viewed using Main Menu > Transport Manager > Maintenance > Transport.

2. If the alarm persists, contact My Oracle Support (MOS).

19407 - Failed to send Transport DATA Message

Event Type: TMF
Description: Failed to send Transport DATA Message
Severity: Info
Instance: <TransportName>, <TransportAdapter>, <TransportProtocol>
**HA Score:** Normal  

**Throttle Seconds:** 10  

**OID:** awptransmgrFailedToSendTransDataMessageNotify  

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

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

   To Troubleshoot:  
   - Check the event history logs at [Main Menu > Alarms & Events > View History](#) for additional SS7 events or alarms from this MP server.  
   - Verify that the adjacent server on the signaling gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.  

2. If the alarm persists, contact [My Oracle Support (MOS)](http://www.oracle.com).  

---  

**19408 - Single Transport Egress-Queue Utilization**  

**Alarm Type:** 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:  

   1. 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.  
   2. 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](#).
3. 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**.

4. 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.

5. 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, contact *My Oracle Support (MOS)*

### 19409 - Message Rejected by ACL Filtering

**Event Type:** TMF  
**Description:** The message is rejected based on configured Access Control List for Transport  
**Severity:** Info  
**Instance:** <TransportName>  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** awptransmgrMessageRejectedByAclFilteringNotify  
**Recovery:**  
1. Verify that the ENUM Server’s IP address is the ACL, or that the ACL is empty.  
2. If the alarm persists, contact *My Oracle Support (MOS)*.

### 19410 - Adjacent Node IP Address state change

**Event Type:** TMF  
**Description:** State change of an IP Address of a multihomed Adjacent Node in SCTP Transport  
**Severity:** Info  
**Instance:** <TransportName>  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** awptransmgrAdjIpAddrStateChangeNotify  
**Recovery:**  
1. Verify that IP network connectivity still exists between the MP server and the adjacent server.  
2. If the alarm persists, contact *My Oracle Support (MOS)*.
19411 - SCTP Transport closed due to failure of multihoming validation

Event Type: TMF
Description: SCTP Transport closed due to failure of multihoming validation
Severity: Info
Instance: <TransportName>
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: awptransmgrSctpTransportRefusedNotify
Recovery:
1. Recheck the Adjacent Node's configure IP Address and validation mode.
2. If alarm persists, contact My Oracle Support (MOS).

19412 - SCTP Transport Transport Configuration Mismatch

Event Type: TMF
Description: IP address advertised by an Adjacent Node in INIT/INIT-ACK chunk are different from configured IP Addresses
Severity: Info
Instance: <TransportName>
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: awptransmgrSctpTransportCfgMismatchNotify
Recovery:
1. Recheck the Configured IP Address and Transport configuration and validation mode.
2. If the alarm persists, contact My Oracle Support (MOS).

19413 - SCTP Transport closed due to unsupported peer type evenet recieved.

Alarm Type: TMF
Description: SCCTP Transport closed due to unsupported add/delete peer IP Address event recieved in Peer Address Notification
Severity: Info
Instance:
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: awptransmgrTransportClosedDueToUnsupportedEventNotify

E53474 Revision 01, July 2014
Recovery:
1. Disable SCTP Dynamic Address Reconfiguration at the Adjacent Node.
2. If the alarm persists, contact My Oracle Support (MOS).

Communication Agent, ComAgent (19800-19909)

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

19800 - Communication Agent Connection Down

Alarm Type: CAF
Description: 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.
Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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. Contact My Oracle Support (MOS) for assistance.

19801 - Communication Agent Connection Locally Blocked

**Alarm Type:** 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

**HA Score:** Normal

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

**OID:** cAFConnLocalBlockedNotify

**Recovery:**

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.

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. Contact My Oracle Support (MOS) for assistance.
19802 - Communication Agent Connection Remotely Blocked

Alarm Type: 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
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: cAFConnRemoteBlockedNotify

Recovery:
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.

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. Contact **My Oracle Support (MOS)** for assistance.

19803 - Communication Agent stack event queue utilization

Alarm Type: CAF

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

**Severity:** Minor, Major, Critical
**Instance:** <ComAgent StackTask Name>
**HA Score:** Normal
**Auto Clear Seconds:** 0 (zero)
**OID:** cAFQueueUtilNotify

**Recovery:**

1. 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. 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.
   
   Contact *My Oracle Support (MOS)* for assistance.

3. If the MP ingres 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.
   
   Contact *My Oracle Support (MOS)* for assistance.

---

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

**Alarm Type:** CAF

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

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

**Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 300 (5 min)

**OID:** cAFClientConnWaitNotify

**Recovery:**
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

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

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. Verify that the remote server is not under maintenance.
5. If the connection is manually disabled at the client MP, and it is expected to be disabled, then no further action is necessary.
6. If the connection has been manually disabled at the client MP, but it is not supposed to be disabled, then enable the connection by clicking on the 'Enable' action button on the Connection Status screen.
7. Verify that IP network connectivity exists between the two connection end-points.
8. Verify that the connection's local IP address and port number are configured on remote client MP.
9. Verify that the Application Process using Communication Agent plug-in is running on both ends.
10. Verify that the connection's remote IP address and port correctly identify remote's listening port.
11. Contact My Oracle Support (MOS) for assistance.

19805 - Communication Agent Failed To Align Connection

Alarm Type: CAF

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)
OID: cAFConnAlignFailedNotify

Recovery:
1. If the connection administrative action is set to ‘disable’, the alarm is cleared. No further action is necessary.
2. Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
3. Find additional information for the alarm in **Main Menu > Alarms & Events > View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
4. Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
5. Check **Main Menu > Communication Agent > Maintenance > Connection Status** to determine which connections on the server have abnormal status.
   For each connection reporting ‘Aligning’ connection status, determine the servers that are endpoints, and verify that the correct software is installed on each server. If incorrect software is present, then server maintenance may be required.
6. Contact **My Oracle Support (MOS)** for assistance.

19806 - Communication Agent CommMessage mempool utilization

**Alarm Type:** CAF

**Description:** The percent utilization of the Communication Agent CommMessage mempool is approaching defined threshold capacity.

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.

**Severity:** Critical, Major, Minor

**Instance:** <ComAgent Process Name>

**HA Score:** Normal

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

**OID:** 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. 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.
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 ingress rate to the server site is exceeding its capacity.
   
   Contact *My Oracle Support (MOS)* for assistance.

19807 - Communication Agent User Data FIFO Queue utilization

**Alarm Type:** CAF

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

**Severity:** Minor, Major, Critical

**Instance:** <ComAgent StackTask Name>

**HA Score:** Normal

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

**OID:** cAFUserDataFIFOUtilNotify

**Recovery:**

1. 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.
   
   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.
   
   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.
   
   Contact *My Oracle Support (MOS)* for assistance.

19808 - Communication Agent Connection FIFO Queue utilization

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

**Severity:** Minor, Major, Critical

**Instance:** <ComAgent StackTask Name>

**HA Score:** Normal

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

**OID:** cAFMxFIFOUtilNotify

**Recovery:**

1. 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.
   
   Contact [My Oracle Support (MOS)](https://support.oracle.com) 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.

   Contact [My Oracle Support (MOS)](https://support.oracle.com) 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.

   Contact [My Oracle Support (MOS)](https://support.oracle.com) for assistance.

---

**19810 - Communication Agent Egress Message Discarded**

**Event Type:** CAF

**Description:** Communication Agent Egress Message Discarded.

**Severity:** Info

**Instance:** < RemoteIp >

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** cAFEventEgressMessageDiscardedNotify

**Recovery:**

1. View the Event AddlInfo column.
Message is being discarded due to one of the reasons specified.

2. If it’s a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.

3. If the event is raised due to software condition, it’s an indication that the Communication Agent Process may be experiencing problems.

4. Use Main Menu > Alarms & Events and examine the alarm log.

5. Contact My Oracle Support (MOS) for assistance.

19811 - Communication Agent Ingress Message Discarded

Event Type: CAF
Description: Communication Agent Ingress Message Discarded.
Severity: Info
Instance: < RemoteIp >
HA Score: Normal
Throttle Seconds: 10
OID: cAFEventIngressMessageDiscardedNotify
Recovery:
1. View the Event AddlInfo column.
   Message is being discarded due to one of the reasons specified.

2. If it’s a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.

3. If the event is raised due to software condition, it is an indication that the Communication Agent Process may be experiencing problems.

4. Use Main Menu > Alarms & Events and examine the alarm log.

5. Contact My Oracle Support (MOS) for assistance.

19814 - Communication Agent Peer has not responded to heartbeat

Event Type: CAF
Description: Communication Agent Peer has not responded to heartbeat.
Severity: Info
Instance: < RemoteIp >
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: cAFEventHeartbeatMissedNotify
Recovery:
1. Check the configuration of managed objects and resolve any configuration issues with the Managed Object or hosting nodes.
   This message may be due to network condition or latency or due to setup issues.

2. If the event is raised due to software condition, it’s an indication that the Communication Agent Process may be experiencing problems.

3. Use Main Menu > Alarms & Events and examine the alarm log.

4. Contact My Oracle Support (MOS) for assistance.

19816 - Communication Agent Connection State Changed

   Event Type: CAF
   Description: Communication Agent Connection State Changed.
   Severity: Info
   Instance: < Remotelp >
   HA Score: Normal
   Throttle Seconds: 0 (zero)
   OID: cAFEventConnectionStateChangeNotify

   Recovery:
   1. Use Main Menu > Alarms & Events and examine the alarm log.
      This Event is a log of connection state change.
   2. 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.
   Severity: Info
   Instance: N/A
   HA Score: Normal
   Throttle Seconds: 0 (zero)
   OID: cAFEventComAgtConfigParamChangeNotify

   Recovery:
   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.
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. 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
   Throttle Seconds: 86400
   OID: cAFDataEvPoolResUtilNotify
   Recovery:
   If the problem persists, contact My Oracle Support (MOS).

19820 - Communication Agent Routed Service Unavailable

   Alarm Type: 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.

19821 - Communication Agent Routed Service Degraded

**Alarm Type:** 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.


19822 - Communication Agent Routed Service Congested

**Alarm Type:** 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 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. Contact My Oracle Support (MOS) for assistance.

---

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

Alarm Type: CAF

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

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSUsingLowPriConnGrpNotify

Recovery:

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

2. Use Main Menu > Communication Agent > Maintenance > Connection Status to view the 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. Contact My Oracle Support (MOS) for assistance.

---

19824 - Communication Agent Pending Transaction Utilization

Alarm Type: CAF

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

Severity: Minor, Major, Critical

Instance: n/a (ComAgent process)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTransUtilNotify
Recovery:

1. 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. Contact **My Oracle Support (MOS)** for assistance.

19825 - Communication Agent Transaction Failure Rate

**Alarm Type:** CAF

**Description:** The number of failed transactions during the sampling period has exceeded configured thresholds.

**Severity:** Minor, Major, Critical

**Instance:** <ServiceName>

**HA Score:** Normal

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

**OID:** cAFTransFailRateNotify

Recovery:

1. 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. Contact **My Oracle Support (MOS)** for assistance.

19826 - Communication Agent Connection Congested

**Alarm Type:** CAF
**Description:** 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.

**Severity:** Major

**Instance:** N/A

**HA Score:** Normal

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

**OID:** 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. Contact **My Oracle Support (MOS)** for assistance.

---

**19830 - Communication Agent Service Registration State Change**

**Event Type:** CAF

**Description:** Communication Agent Service Registration State Change.

**Severity:** Info

**Instance:** <ServiceName>

**HA Score:** Normal

**Throttle Seconds:** 0 (zero)

**OID:** cAFEventComAgtSvcRegChangedNotify

**Recovery:**

This event is a log of normal application startup and shutdown activity. It may provide aid during trouble shooting 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
Throttle Seconds: 0 (zero)
OID: cAFEventComAgtSvcOpStateChangedNotify
Recovery:
1. This event indicates that a Communication Agent service changed operational state, and typically results from maintenance actions.
   A service can also change state due to server overload.
2. If the state change is unexpected, then 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: cAFEventComAgtTransFailedNotify
Recovery:
1. Use Main Menu > Communication Agent > Maintenance > Connection Status to determine if the local server is unable to communicate with another server or if servers have become overloaded.
2. Check the server’s KPIs and the Main Menu > Communication Agent > Maintenance > Connection Status to trouble-shoot the cause of server overload.
3. Check the Main Menu > Communication Agent > Maintenance > HA Status that corresponds to the ServiceID in the event instance to trouble-shoot the operation of the service.
4. If the event cannot be explained by maintenance actions, then Contact My Oracle Support (MOS) for assistance.
19833 - Communication Agent Service Egress Message Discarded

Event Type: CAF
Description: Communication Agent Service Egress Message Discarded.
Severity: Info
Instance: <ServiceName>, <RemoteIP> | <null>
• If serviceID is unknown, then <ServiceName> is null.
HA Score: Normal
Throttle Seconds: 10
OID: cAFEventRoutingFailedNotify
Recovery:
1. View the Event AddlInfo column.
   Message is being discarded due to one of the reasons specified.
2. If it’s a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, It’s an indication that the Communication Agent Process may be experiencing problems.
4. Use Main Menu > Alarms & Events and examine the alarm log.
5. Contact My Oracle Support (MOS) for assistance.

19842 - Communication Agent Resource-Provider Registered

Event Type: CAF
Description: Communication Agent Resource-Provider Registered.
Severity: Info
Instance: <ResourceName>
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: cAFEventResourceProviderRegisteredNotify
Recovery:
No action required.

19843 - Communication Agent Resource-Provider Resource State Changed

Event Type: CAF
Description: Communication Agent Resource-Provider Resource State Changed.
Severity: Info
19844 - Communication Agent Resource-Provider Stale Status Received

Event Type: CAF
Description: Communication Agent Resource-Provider Stale Status Received.
Severity: Info
Instance: <ProviderServerName>: <ResourceName>
HA Score: Normal
Throttle Seconds: 10
OID: cAFEventStaleHBPacketNotify
Recovery:
   If this event is occurring frequently then check the ComAgent maintenance screens for other anomalies and to troubleshoot further.

19845 - Communication Agent Resource-Provider Deregistered

Event Type: CAF
Description: Communication Agent Resource-Provider Deregistered.
Severity: Info
Instance: <ResourceName>
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: cAFEventResourceProviderDeRegisteredNotify
Recovery:
   No action required.

19846 - Communication Agent Resource Degraded

Alarm Type: CAF
Description: Communication Agent Resource Degraded. A local application is using the resource, identified in the alarm, and the access to the resource is impaired. Some of the resource providers are either unavailable and/or congested.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFResourceCongestedNotify

Recovery:

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

2. Use Main Menu > Communication Agent > Maintenance > Connection Status to determine if connections have failed or have congested.

3. Contact My Oracle Support (MOS) for assistance.

19847 - Communication Agent Resource Unavailable

Alarm Type: CAF

Description: Communication Agent Resource Unavailable. A local application needs to use a ComAgent resource, but the resource is unavailable. The resource can be unavailable if the local server has no ComAgent connections to servers providing the resource or no servers host active instances of the resource’s sub-resources.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFResourceUnavailNotify

Recovery: Check the Communication Agent Connection Status maintenance screen

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. Contact My Oracle Support (MOS) for assistance.
### 19848 - Communication Agent Resource Error

**Alarm Type:** CAF  
**Description:** Communication Agent Resource Error. Two sets of servers are using incompatible configurations for a ComAgent resource.  
**Severity:** Minor  
**Instance:** `<ResourceName>`  
**HA Score:** Normal  
**Auto Clear Seconds:** 50  
**OID:** `cAFResourceErrorNotify`  
**Recovery:**  
1. Use **Main Menu > Communication Agent > Maintenance > HA Services Status** to determine which sets of servers are incompatible.  
   Check the incompatible servers to verify that they are operating normally and are running the expected versions of software.  
2. Contact **My Oracle Support (MOS)** for assistance.

### 19850 - Communication Agent Resource-User Registered

**Event Type:** CAF  
**Description:** Communication Agent Resource-User Registered.  
**Severity:** Info  
**Instance:** `<ResourceName>`  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** `cAFEventResourceUserRegisteredNotify`  
**Recovery:**  
   No action required.

### 19851 - Communication Agent Resource-User Deregistered

**Event Type:** CAF  
**Description:** Communication Agent Resource-User Deregistered.  
**Severity:** Info  
**Instance:** `<ResourceName>`  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)
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
Throttle Seconds: 1
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 AddlInfo.
   If the condition is persistent with the status of one of the ComAgent Configuration Managed Objects there is an underlying issue with the Managed Object.
2. Use Main Menu > Alarms & Events and examine the alarm log for ComAgent Process problems.
3. Contact My Oracle Support (MOS) for assistance.

19854 - Communication Agent Resource-Provider Tracking Table Audit Results

Event Type: CAF
**Communication Agent Resource-Provider Tracking Table Audit Results.** This event is generated when a Resource Provider Tracking Table (RPTT) entry with Status equal to Auditing is replaced with a new status (null, Active, Standby, Spare, OOS, etc) and there are no other RPTT entries, for this specific Resource/SR, with Status equal to Auditing.

**Severity:** Info  
**Instance:** None  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** cAFEventHaRPTTAuditResultNotify  
**Recovery:**  
No action required.

### 19855 - Communication Agent Resource Has Multiple Actives

**Alarm Type:** CAF  
**Description:** This alarm indicates a possible IP network disruption that has caused more than one Resource Provider to become Active. The server that asserted this alarm expects there to be only one active Resource Provider server for the Resource, but instead it is seeing more than one. During this condition the server may be sending commands to the wrong Resource Provider. This may affect applications such as CPA, PDRA.  
**Severity:** Major  
**Instance:** <ResourceName>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** cAFMultipleActivesNotify  
**Recovery:**  
1. Use Main Menu > Communication Agent > Maintenance > HA Services Status to determine which Resource Provider servers are announcing ‘Active’ status for the Resource.  
2. Investigate possible IP network isolation between these Resource Provider servers.  
3. Contact My Oracle Support (MOS) for assistance.

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

**Event Type:** CAF  
**Description:** The Communication Agent Service Provider Registration State has changed.  
**Severity:** Info  
**Instance:** <ServiceName>  
**HA Score:** Normal  
**Throttle Seconds:** 1
OID: cAFEventSvcProvRegStateChangedNotify

Recovery:
1. This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.
2. Contact My Oracle Support (MOS) for further assistance.

19857 - Communication Agent Service Provider Operational State Changed

Event Type: CAF
Description: The Communication Agent Service Provider Operational State has Changed
Severity: Info
Instance: <ServiceName>
HA Score: Normal
Throttle Seconds: 1
OID: cAFEventSvcProvOpStateChangedNotify

Recovery:
1. This event indicates that a ComAgent service provider changed operational state, and typically results from maintenance actions. A service can also change state due to overload.
2. If the state change is unexpected, contact My Oracle Support (MOS).

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group: CAF
Description: The maximum number of connections per connection group limit has been reached.
Severity: Info
Instance: <Connection group name>
HA Score: Normal
Throttle Seconds: 86400
OID: cAFComAgentMaxConnsInConnGrpNotify

Recovery:
1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.
2. Contact My Oracle Support (MOS) for further assistance.

19860 - Communication Agent Configuration Daemon Table Monitoring Failure

Alarm Type: CAF
Description: This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTableMonitorFailureNotify

Recovery:

1. Use 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, then 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, then Contact My Oracle Support (MOS) for assistance.

19861 - Communication Agent Configuration Daemon Script Failure

Alarm Type: CAF

Description: This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 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, then 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, then 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 hardware, 75k on other hardware
- Major - if exceeding 110K on Gen8 hardware, 80k on other hardware
- Critical - if exceeding 120K on Gen8 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. Contact My Oracle Support (MOS) for further assistance.

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group: CAF

Description: The maximum number of connections per connection group limit has been reached.

Severity: Info

Instance: <Connection group name>

HA Score: Normal

Throttle Seconds: 86400
**OID:** cAFComAgentMaxConnsInConnGrpNotify

**Recovery:**

1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.
2. Contact *My Oracle Support (MOS)* for further assistance.

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

**Event Group:** CAF  
**Description:** ComAgent successfully set the host server hardware profile.  
**Severity:** Info  
**Instance:** None  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** cAFEventSuccessSetHostServerHWProfileNotify  

**Recovery:**

1. This event indicates that all TPS controlling parameter values are successfully set for the host server hardware profile.  
2. If needed, contact *My Oracle Support (MOS)*.

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

**Event Group:** CAF  
**Description:** ComAgent failed to set the host server hardware profile.  
**Severity:** Info  
**Instance:** None  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)  
**OID:** cAFEvetFailToSetHostServerHWProfileNotify  

**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, contact *My Oracle Support (MOS)*.

**19900 - Process CPU Utilization**

**Alarm Type:** 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.
   Contact My Oracle Support (MOS) for assistance.

19901 - CFG-DB Validation Error

Alarm Type: STK

Description: A minor database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbValidationErrorNotify

Recovery:
   An unexpected condition has occurred while performing a database update, but database updates are still enabled.
   Contact My Oracle Support (MOS) for assistance.

19902 - CFG-DB Update Failure

Alarm Type: STK
Description: A critical database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are DISABLED.

Severity: Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: dbcCfgDbUpdateFailureNotify
Recovery:
   An unexpected condition has occurred while performing a database update and database updates are disabled.
   Contact My Oracle Support (MOS) for assistance.

19903 - CFG-DB post-update Error

Alarm Type: STK

Description: A minor database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: dbcCfgDbPostUpdateErrorNotify
Recovery:
   An unexpected condition has occurred while performing a database update, but database updates are still enabled.
   Contact My Oracle Support (MOS) for assistance.

19904 - CFG-DB post-update Failure

Alarm Type: 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.
   Contact My Oracle Support (MOS) for assistance.

19905 - Measurement Initialization Failure
   Alarm Type: 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.
      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
   Event Type: DIAG
   Description: Normal traffic is being discarded because it is routed to an egress Test Connection. An
egress Test Connection is given a normal message to be transmitted.
   Severity: Major
   Instance: <Connection name>
   HA Score: Normal
Throttle Seconds: 86400
OID: dbcNormalMessageDiscardedNotify
Recovery:
1. Update routing rules to exclude Test connections from being used for routing.
   Normal traffic should be received and sent on non-test connections.
2. Change the hostname of the peer connected to the test connection.
   The hostname of the peer connected to the test connection may be the destination host for the
   incoming normal traffic.

19911 - Test message discarded

Event Type: DIAG
Description: Test message is given to a non-test connection to be transmitted.
Severity: Info
Instance: <Connection name>
HA Score: Normal
Throttle Seconds: 5
OID: dbcDiagnosticMessageDiscardNotify
Recovery:
   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 (22000-22350, 22900-22999)

22001 - Message Decoding Failure

Event Type: DIAM
Description: A message received from a peer was rejected because of a decoding failure. Decoding
failures can include missing mandatory parameters. A Diameter message was received either without
the mandatory Destination-Realm AVP or, while parsing the message, the message content was
inconsistent with the Message Length in the message header.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterIngressMsgRejectedDecodingFailureNotify

Recovery:

These protocol violations are 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 (identified by the Peer Name) and cannot be fixed using the application.

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.

22003 - Application ID Mismatch with Peer

Event Type: DIAM

Description: While attempting to route a request message to a peer, a peer’s transport connection was bypassed because the peer did not support the Application ID for that transport connection.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterApplicationIdMismatchWithPeerNotify

Recovery:

1. The system’s peer routing table may be using a Route List containing a peer which does not support the Application ID or the list of Application IDs supported by the peer on each connection may not be the same. The list of Application IDs that the peer supports on each connection can be viewed as follows:
   a) Navigate to the GUI page: 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 the GUI page: Diameter > Maintenance > Connections
   b) Locate the relevant Connection
   c) Disable the Connection
   d) Enable the Connection

3. The Diameter Node which originated the message (identified by the Origin-Host AVP) could be configured incorrectly and the application is trying to address a node which doesn't support the Application ID. This cannot be fixed using this application.

4. If the problem persists, contact My Oracle Support (MOS).

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. Contact My Oracle Support (MOS) for assistance.

22005 - No peer routing rule found

Event Type: DIAM
Description: A message not addressed to a peer (either Destination-Host AVP was absent or Destination-Host AVP was present but was not a peer's FQDN) could not be routed because no Peer Routing Rules matched the message.
Severity: Info
Instance: <MPName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterNoPrtRuleNotify
Recovery:
1. Either the message was incorrectly routed to this node or additional Peer Routing Rules need to be added. Existing Peer Routing Rules can be viewed and updated using Diameter > Configuration > Peer Routing Rules page.
2. If the problem persists, contact My Oracle Support (MOS).

22006 - Forwarding Loop Detected

Event Type: DIAM
Description: The Ingress Request message received was previously processed by the local node as determined from the Route-Record AVPs received in the message.
Severity: Info
Instance: <PeerName>
HA Score: Normal
Throttle Seconds: 10
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 incorrectly routing the message and the issue cannot be fixed using this application.
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, contact My Oracle Support (MOS).

22007 - Inconsistent Application ID Lists from a Peer

Event Type: DIAM
Description: The list of Application IDs supported by a peer during the Diameter Capabilities Exchange procedure on a particular transport connection is not identical to one of the list of Application IDs received from the peer over a different available transport connection to that peer.
Severity: Info
Instance: <PeerName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterSupportedAppIdsInconsistentNotify
Recovery:
1. A peer with multiple transport connections has established a connection and provided a list of supported Application IDs which does match a previously established connection. This could
prevent Request messages from being routed uniformly over the peer's transport connections because the decision to route a message containing an Application ID is based upon the list of Application IDs supported on each transport connection. The list of Application IDs that the peer supports on each connection can be viewed as follows:

a) Navigate to **Diameter > Maintenance > Connections**.
b) Locate the relevant Peer Node and check the supported Application IDs.

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

a) Navigate to **Diameter > Maintenance > Connections**.
b) Locate the relevant Connection.
c) Disable the Connection.
d) Enable the Connection.

3. If the problem persists, contact **My Oracle Support (MOS)**.

### 22008 - Orphan Answer Response Received

**Event Type:** DIAM  
**Description:** An Answer response was received for which no pending request transaction existed, resulting in the Answer message being discarded. When a Request message is forwarded the system saves a pending transaction, which contains the routing information for the Answer response. The pending transaction is abandoned if an Answer response is not received in a timely fashion.  
**Severity:** Info  
**Instance:** <TransConnName>  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterOrphanAnswerResponseReceivedNotify  
**Recovery:**  
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 **Diameter > Configuration > System Options** page.

### 22009 - Application Routing Rules with Same Priority

**Event Type:** DIAM  
**Description:** An application routing table search with a received Request message found more than one highest priority application routing rule match. At least two application routing rules with the same priority matched an ingress Request message. The system selected the first application routing rule found.  
**Severity:** Info  
**Instance:** <MPName>  
**HA Score:** Normal  
**Throttle Seconds:** 10
OID: eagleXgDiameterApplicationRoutingTableRulesSamePriorityNotify

Recovery:
1. It is recommended that application routing rules be unique for the same type of messages to avoid unexpected routing results. Peer routing rule priorities can be modified using Diameter > Configuration > Application Routing Rules page.
2. If the problem persists, 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
OID: eagleXgDiameterSpecifiedDasRouteListNot ProvisionedNotify

Recovery:
1. Provisioning is incorrect/misconfigured. Verify provisioning and provision/correct provisioning.
2. If this problem persists, contact My Oracle Support (MOS) for assistance.

22012 - Specified MCCS not provisioned

Event Type: DIAM
Description: The Message copy CfgSet attached to the original message by the trigger point is not provisioned
Severity: Info
Instance: <MCCS>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterSpecifiedMCCSNot ProvisionedNotify

Recovery:
1. Verify the configured value of MCCS with the trigger point.
2. Verify the Message Copy CfgSet (MCCS) provisioning is properly configured.
3. If the problem persists, contact My Oracle Support (MOS).

22013 - DAS Peer Number of Retransmits Exceeded for Copy

Event Type: DIAM
Description: The configured number of Message Copy retransmits has been exceeded for the DAS Peer.

Severity: Info

Instance: <MCCS>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterNumberOfRetransmitsExceededToDasNotify

Recovery:
1. Verify the configured value of 'Max Retransmission Attempts'
2. Verify local provisioning to connections to intended DAS peer server(s) are in service and no network issues in path(s) to intended DAS peer server(s) exist.
3. Verify DAS peer provisioning to insure proper configuration.
4. If the problem persists, contact My Oracle Support (MOS) for assistance.

22014 - No DAS Route List specified

Alarm Type: DIAM

Description: No valid DAS Route List was specified in the Message Copy Config Set.

Severity: Info

Instance: <RouteListId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterNoDasRouteListSpecifiedNotify

Recovery:
Contact the My Oracle Support (MOS) for further assistance.

22015 - Connection Operational Status Inconsistency May Exist

Event Type: DIAM

Description: DSR was unable to update the Operational Status and Operation Reason attributes for a transport connection on the OAM.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterOperationalStatusInconsistencyNotify

Recovery:
1. Use Main Menu > Diameter > Maintenance > Connections to view the Operational Status and Operation Reason attributes for a Connection.

The Operational Status and Operation Reason attributes for a Connection on the OAM may be temporarily out of date with the values on DSR.

This occurs when an internal event queue size has been exceeded. This should rarely occur and the inconsistency should be cleared when the Connection’s “Remote Busy State” changes again.

2. If the problem persists, contact My Oracle Support (MOS).

22016 - Peer Node Alarm Aggregation Threshold

Alarm Type: DIAM

Description: This alarm occurs when there are a ‘Critical’ number of Peer Node alarms for a single Network Element.

Note: The Alarm Thresholds are configurable using the “Alarm Threshold Options” tab on the Main Menu > Diameter > Configuration > System Options screen.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 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. Contact My Oracle Support (MOS) for assistance.

22017 - Route List Alarm Aggregation Threshold

Alarm Type: DIAM

Description: This alarm occurs when there are a ‘Critical’ number of Route List alarms for the Network Element.

Note: The Alarm Thresholds are configurable using the “Alarm Threshold Options” tab on the Main Menu > Diameter > Configuration > System Options screen.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListUnavailableThresholdReachedNotify
Recovery:
1. Use Main Menu > Diameter > Maintenance > Route Lists to monitor Route List status.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List are not under maintenance.
5. Contact My Oracle Support (MOS) for assistance.

22018 - Maintenance Leader HA Notification to go Active

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

22019 - Maintenance Leader HA Notification to go OOS

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

22020 - Copy Message size exceeded the system limit

Event Type: DIAM
Description: The size of the message being copied to the DAS exceeded the maximum message size set system wide.
Severity: Info
Instance: <DA-MP>
HA Score: Normal
Throttle Seconds: 10
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, contact My Oracle Support (MOS) for assistance.

22021 - Debug Routing Info AVP Enabled

Event Type: DIAM
Description: Debug Routing Info AVP is enabled.
Severity: Minor
Instance: None
HA Score: Normal
Throttle Seconds: 86400
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, contact My Oracle Support (MOS).

22051 - Peer Unavailable

Alarm Type: DIAM
Description: Unable to access the Diameter Peer because all of the transport connections are Down.
Severity: Critical
Instance: <PeerName> (of the Peer which failed)
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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, contact My Oracle Support (MOS).

22052 - Peer Degraded

Alarm Type: DIAM
Description: The peer has some available connections, but less than its minimum connection capacity. Continued routing to this peer may cause congestion or other overload conditions.
Severity: Major
Instance: <PeerName> (of the Peer which is degraded)
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterPeerDegradedNotify

Recovery:
1. Peer status can be monitored from Diameter > Maintenance > Peer Nodes.
2. Verify 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, contact My Oracle Support (MOS).

22053 - Route List Unavailable

Alarm Type: DIAM
Description: 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.

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: Critical
Instance: <RouteListName> (of the Route List which failed)
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterRouteListUnavailableNotify

Recovery:
1. Route List status can be monitored from Diameter > Maintenance > Route Lists.
2. Verify 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, contact My Oracle Support (MOS).

22054 - Route List Degraded

Alarm Type: DIAM

Description: The Route List’s Operational Status has changed to Degraded because the capacity of the Route List’s Active Route Group has dropped below the Route List’s configured minimum capacity. There are two potential causes:

1. One or more of the Route List’s peers become Unavailable. A Peer becomes Unavailable when all of its transport connections become Unavailable. If a Transport Connection is configured for Initiate mode, the Network Element 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.
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, contact My Oracle Support (MOS).

22055 - Non-Preferred Route Group in Use

Alarm Type: 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, contact My Oracle Support (MOS).

22057 - Egress Throttle Group Rate Limit Degraded

Alarm Type: DIAM

Description: The ETG Rate Limit has exceeded the defined threshold

Severity: Major

Instance: <ETGName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgRateLimitDegradedNotify

Recovery:

1. Check the configuration in 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, contact My Oracle Support (MOS).

22058 - Egress Throttle Group Pending Transaction Limit Degraded

Alarm Type: DIAM
Description: The ETG Pending Transactions Limit has exceeded the defined threshold

Severity: Major

Instance: <ETGName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgPendingTransLimitDegradedNotify

Recovery:
1. Check the configuration in **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, contact **My Oracle Support (MOS)**.

22059 - Egress Throttle Group Message Rate Congestion Level changed

Event Group: DIAM

Description: The Egress Throttle Group Message rate Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity: N/A

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. 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:** N/A  
**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, contact **My Oracle Support (MOS)** for assistance.

**22061 - Egress Throttle Group Monitoring stopped**

**Alarm Type:** DIAM  
**Description:** ETG Rate and Pending Transaction Monitoring is stopped on all configured ETGs  
**Severity:** Minor  
**Instance:** <DA-MP Hostname>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterEtgMonitoringStoppedNotify  
**Recovery:**  
1. Verify 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, contact My Oracle Support (MOS).

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

**Event Type:** Diameter  
**Description:** Topology Hiding could not be applied because the Actual Host Name could not be determined  
**Severity:** N/A  
**Instance:** <CfgSetName>  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterTopoHidingActualHostNameNotFoundNotify  
**Recovery:**
1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set.
2. If any DSR Applications are activated on DSR, ensure that any specific Application Level Topology Hiding feature is not conflicting with the contents of Actual Host Names specified in the MME Configuration Set.
3. Check if the first instance of a Session-ID AVP in the Request/Answer message contains the mandatory delimited ";".
4. If the problem persists, contact My Oracle Support (MOS).

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

**Event Type:** DIAM  
**Description:** The size of the message encoded by DSR has exceeded its max limits  
**Severity:** Info  
**Instance:** <TransConnName>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterDiameterMaxMsgSizeLimitExceededNotify  
**Recovery:**
No action required. However, if this event is seen to be incrementing consistently, contact My Oracle Support (MOS) for assistance.

**22101 - Connection Unavailable**

**Alarm Type:** 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:** `<TransConnName>`

**HA Score:** Normal

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

**OID:** eagleXgDiameterConnectionUnavailableAlarmNotify

**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, contact *My Oracle Support (MOS)*.

---

**22102 - Connection Degraded**

**Alarm Type:** 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:** `<TransConnName>`

**HA Score:** Normal

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

**OID:** eagleXgDiameterConnectionDegradedAlarmNotify

**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 Connection Impaired**

**Alarm Type:** DIAM

**Description:** One or more paths of the SCTP connection went down.

**Severity:** Minor

**Instance:** `<TransConnName>`

**HA Score:** Normal

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

**OID:** eagleXgDiameterSCTPConnectionImpairedAlarmNotify
Recovery:
1. Identify the most recent SCTP Connection Impaired event in the event log for the connection and use the Event’s recovery steps to resolve the issue.
2. If the problem persists, contact My Oracle Support (MOS).

22104 - SCTP peer is operating with a reduced IP address set

Alarm Type: DIAM
Description: The SCTP peer advertised less IP addresses than desired by the connection configuration. If two IP addresses have been configured for the Local Node of a certain SCTP connection, but following the SCTP connection establishment the peer node has advertised only one IP address (basically less than the number of IP addresses configured for the local node).
Severity: Minor
Instance: <TransConnName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterSCTPPeerReducedIPSetAlarmNotify
Recovery:
1. The peer is not able to advertise more than one IP address either due to an error in its configuration or due to being affected by a network interface failure. Check the networking configuration on the peer node.
2. If the problem persists, contact My Oracle Support (MOS).

22106 - Ingress Message Discarded: DA-MP Ingress Message Rate Control

Alarm Type: DIAM
Description: An ingress message is discarded due to connection (or DA-MP) ingress message rate exceeding connection (or DA-MP) maximum ingress MPS.
Severity: Major
Instance: <MPHostName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterIngressMessageDiscardedAlarmNotify
Recovery:
1. The ingress MPS on the DA-MP is exceeding the MP Maximum Ingress MPS. Consider decreasing the overall ingress message rate on the DA-MP by diverting the traffic or reducing the traffic.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.
22200 - Local MP Congestion

**Alarm Type:** DIAM  
**Description:** The Diameter Process is approaching or exceeding its engineered traffic handling capacity.  
**Severity:** Minor, Major, Critical  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterLocalMpCongestionNotify

**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).

22201 - Ingress Message Rate

**Alarm Type:** DIAM  
**Description:** The ingress message rate for the MP is approaching or exceeding its engineered traffic handling capacity.  
**Severity:** Minor, Major, Critical  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterIngressMsgRateNotify

**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, contact My Oracle Support (MOS).

22202 - PDU Buffer Pool Utilization

Alarm Type: DIAM

Description: 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. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPduBufferPoolUtilNotify

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, contact My Oracle Support (MOS).

22203 - PTR Buffer Pool Utilization

Alarm Type: DIAM

Description: The MP’s PTR buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterPtrBufferPoolUtilNotify

Recovery:
1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the Status & Manage > Server page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the Status & Manage > KPIs page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the Status & Manage > KPIs page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined from the Alarms & Events page.
5. If the problem persists, contact My Oracle Support (MOS).

22204 - Request Message Queue Utilization

Alarm Type: DIAM
Description: The MP’s Request Message Queue Utilization is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress Request messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.
Severity: Minor, Major, Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterRequestMessageQueueUtilNotify

Recovery:
1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the Status & Manage > Server page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the Status & Manage > KPIs page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the Status & Manage > KPIs page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the Request Task may be experiencing a problem preventing it from processing messages from its Request Message Queue. The alarm log should be examined from the **Alarms & Events** page.

5. If the problem persists, contact **My Oracle Support (MOS)**.

### 22205 - Answer Message Queue Utilization

**Alarm Type:** DIAM  
**Description:** The MP’s Answer Message Queue Utilization is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress Answer messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.  
**Severity:** Minor, Major, Critical  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterAnswerMessageQueueUtilNotify  
**Recovery:**
1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage > Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage > KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage > KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the Answer Task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. The alarm log should be examined from the **Alarms & Events** page.
5. If the problem persists, contact **My Oracle Support (MOS)**.

### 22206 - Reroute Queue Utilization

**Alarm Type:** DIAM  
**Description:** The MP’s Reroute Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization any transactions requiring rerouting will be rejected. This alarm should not normally occur when no other congestion alarms are asserted.  
**Severity:** Minor, Major, Critical  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)
OID: eagleXgDiameterRerouteQueueUtilNotify

Recovery:
1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer time-outs. The status of connections should be examined from the Diameter > Maintenance > Connections page.
2. If no additional congestion alarms are asserted, the Reroute Task may be experiencing a problem preventing it from processing messages from its Reroute Queue. The alarm log should be examined using the Alarms & Events page.
3. If the problem persists, contact My Oracle Support (MOS).

22207 - All-Connections Event Queue Utilization

Alarm Type: DIAM
Description: The MP’s All-Connections Event Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress transactions will be rejected. This alarm should not normally occur when no other congestion alarms are asserted.
Severity: Minor, Major, Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterAllConnEventQueueUtilNotify

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 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 task may be experiencing a problem preventing it from processing events from its All-Connections Event Queue. The alarm log should be examined using the Alarms & Events page.
5. If the problem persists, contact My Oracle Support (MOS).

22208 - Per-Connection Egress Message Queue Utilization

Alarm Type: DIAM
Description: The MP’s per-connection egress message queue is approaching its maximum capacity.
Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterPerConnMessageQueueUtilNotify
Recovery: 
Contact My Oracle Support (MOS) for further assistance.

22209 - Message Copy Disabled

Alarm Type: 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 Type: DIAM
Description: The 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. 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. Examine the alarm log from **Main Menu > Alarms & Events**.
5. If the problem persists, contact *My Oracle Support (MOS).*

---

**22215 - Ingress Message Discarded: DA-MP Overload Control**

**Alarm Type:** DIAM

**Description:** Ingress message is discarded due to DA-MP CPU congestion

**Severity:** Major

**Instance:** MPHostName (Hostname of the DA-MP)

**HA Score:** Normal

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

**OID:** eagleXgDiameterIngressMessageDiscardedOverLoadControlAlarmNotify

**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 DA-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 DA-MP from **Main Menu > Status & Manage > KPIs.** Each DA-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. Monitor the ingress traffic rate of each DA-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.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu > Alarms & Events.**
5. If the problem persists, contact *My Oracle Support (MOS).*
22216 - Ingress Message Discarded: Priority 0 message discarded by DA-MP Overload Control

Alarm Type: DIAM
Description: Ingress Priority 0 message discarded due to DA-MP CPU congestion.
Severity: Info
Instance: MPHostName (Hostname of the DA-MP)
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterMpIngressPri0MessageDiscardedNotify

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.
4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.
5. If the problem persists, contact My Oracle Support (MOS).

22217 - Ingress Message Discarded: Priority 1 message discarded by DA-MP Overload Control

Alarm Type: DIAM
Description: Ingress Priority 1 message discarded due to DA-MP CPU congestion.
Severity: Info
Instance: MPHostName (Hostname of the DA-MP)
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterMpIngressPri1MessageDiscardedNotify

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.

4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

22218 - Ingress Message Discarded: Priority 2 message discarded by DA-MP Overload Control

<table>
<thead>
<tr>
<th>Alarm Type: DIAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: Ingress Priority 2 message discarded due to DA-MP CPU congestion.</td>
</tr>
<tr>
<td>Severity: Info</td>
</tr>
<tr>
<td>Instance: MPHostName (Hostname of the DA-MP)</td>
</tr>
<tr>
<td>HA Score: Normal</td>
</tr>
<tr>
<td>Throttle Seconds: 30</td>
</tr>
<tr>
<td>OID: eagleXgDiameterMpIngressPri2MessageDiscardedNotify</td>
</tr>
</tbody>
</table>

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.

4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

22220 - Connection Congestion Level change

<table>
<thead>
<tr>
<th>Event Type: DIAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: The egress congestion level associated with the connection has changed. When a connection's egress queue is congested, the connection's operational status will be Degraded. If this problem persists and the queue reaches 100% utilization all new egress messages for the Connection will be discarded. This event should not normally occur when no other congestion alarms are asserted.</td>
</tr>
</tbody>
</table>
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterConnCongestionLevelChangeNotify
Recovery:
1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the Alarms & Events page.
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. MP server status can be monitored using the Status & Manage > Server page.
4. 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 using the Status & Manage > KPIs page. 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. The ingress traffic rate of each MP can be monitored using 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.
6. If the problem persists, contact My Oracle Support (MOS).

22221 - Routing MPS Rate

Alarm Type: 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, contact *My Oracle Support (MOS)*.

### 22222 - Long Timeout PTR Buffer Pool Utilization

**Alarm Type:** DIAM  
**Description:** The MP’s Long Timeout PTR buffer pool is approaching its maximum capacity.  
**Severity:** Minor, Major, Critical  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterLongTimeoutPtrBufferPoolUtilNotify  
**Recovery:**

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **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, contact *My Oracle Support (MOS)*.

### 22223 - DA-MP Memory Utilization Exceeded

**Alarm Type:** DIAM  
**Description:** DA-MP memory utilization has exceeded its configured limits.
Severity: Minor, Major, Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDaMpMemUtilizationExceededNotify
Recovery:

1. MPS exceeding its configured limits. Alarm 22221 - Routing MPS Rate will be raised; perform the Recovery steps for this alarm.
2. Average hold time exceeding its configured limits. Alarm 22224 - Average Hold Time Limit Exceeded will be raised. Perform the Recovery steps for this alarm.
3. Average message size exceeding its configured limits. Alarm 22225 - Average Message Size Limit Exceeded will be raised. Perform the Recovery steps for this alarm.
4. Other. If the DA-MP is not exceeding any of the limits specified above, contact Oracle for assistance.

22224 - Average Hold Time Limit Exceeded
Alarm Type: DIAM
Description: The average transaction hold time has exceeded its configured limits.
Severity: Minor, Major, Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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 - Average Message Size Limit Exceeded
Alarm Type: DIAM
Description: The size of the average message processed by DSR has exceeded its configured limits.
Severity: Minor, Major, Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterAvgMsgSizeLimitExceededNotify
Recovery:
The size of the average message processed by DSR is exceeding its configured limits. This may cause DSR to consume an abnormally large amount of memory, leading to performance degradation. Alarm 22223 - DA-MP Memory Utilization Exceeded may be raised as a result. Examine the traffic coming from connected peers to see if any of them are sending abnormally large messages.

22300 - Connection Unavailable: Socket configuration failure

  Event Type: DIAM
  Description: Software failure attempting to configure SCTP or TCP socket.
  Severity: Info
  Instance: TransConnName
  HA Score: Normal
  Throttle Seconds: 30
  OID: eagleXgDiameterConnUnavailSocketCfgFailureNotify
  Recovery:
    Contact My Oracle Support (MOS).

22301 - Connection Unavailable: Connection initiation failure

  Event Type: DIAM
  Description: Failure occurred while attempting to initiate SCTP or TCP connection with the peer.
  Severity: Info
  Instance: TransConnName
  HA Score: Normal
  Throttle Seconds: 30
  OID: eagleXgDiameterConnUnavailConnInitFailureNotify
  Recovery:
    1. Confirm that connection is not administratively Disabled at the peer.
    2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches local connection configuration.
    3. Confirm IP network connectivity between peer IP and local IP for the connection.
    4. 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.
    5. If the problem persists, contact My Oracle Support (MOS).

22302 - Connection Unavailable: Received malformed message

  Event Type: DIAM
Description: Diameter message received from peer with invalid or inconsistent header/AVP length fields.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedMalformedMessageNotify

Recovery:
1. Determine if other nodes/MPs connected to the peer are also experiencing problems with messages received from the peer. If so, the peer should be diagnosed.
2. Determine if other connections on this same MP are also experiencing problems. If so, the MP should be removed moved from service, replaced, and the My Oracle Support (MOS) should be contacted to assist with resolution.

22303 - Connection Unavailable: Peer closed connection

Event Type: DIAM

Description: The SCTP or TCP connection was closed by the peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailPeerClosedConnNotify

Recovery:
1. If unexpected, use peer node diagnostic/log information to determine why peer closed connection.
2. If the problem persists, contact My Oracle Support (MOS).

22304 - Connection Unavailable: Proving Failure

Event Type: DIAM

Description: Connection closed after DWR/DWA based proving algorithm failure.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailProvingFailureNotify

Recovery:
1. Examine the peer to determine why it is not responding to DWRs.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 22305 - Connection Admin State change

**Event Type:** DIAM  
**Description:** The Administrative state of the connection has changed.  
**Severity:** Info  
**Instance:** TransConnName  
**HA Score:** Normal  
**Throttle Seconds:** 1  
**OID:** eagleXgDiameterConnectionAdminStateChangeNotify  
**Recovery:**  
No action required.

### 22306 - Connection Unavailable: Timeout waiting for CER/CEA

**Event Type:** DIAM  
**Description:** Connection closed after Tcex timer expired while waiting on CER or CEA from peer.  
**Severity:** Info  
**Instance:** TransConnName  
**HA Score:** Normal  
**Throttle Seconds:** 1  
**OID:** eagleXgDiameterConnUnavailTimedOutWaitingForCexNotify  
**Recovery:**  
1. For peer initiated connections, confirm that the configured Tcex timer value is not configured to be less than the expected time for peer to send CER after successfully initiating connection.  
2. For locally initiated connections, confirm that the configured Tcex timer value is not less than the time expected for the peer to respond with CEA after receiving CER.  
3. If the problem persists, contact *My Oracle Support (MOS)*.

### 22307 - Connection Unavailable: Timeout waiting for DPA

**Event Type:** DIAM  
**Description:** Connection closed after Tdpa timer expired while waiting on DPA from peer.  
**Severity:** Info  
**Instance:** TransConnName  
**HA Score:** Normal
22308 - Received Unexpected CER/CEA

Event Type: DIAM
Description: CER or CEA message was received from the peer when it was not expected.
Severity: Info
Instance: TransConnName
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterReceivedUnexpectedCexNotify
Recovery:
1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact My Oracle Support (MOS).

22309 - Received Unexpected DWR/DWA

Event Type: DIAM
Description: DWR or DWA message was received from the peer when it was not expected.
Severity: Info
Instance: TransConnName
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterReceivedUnexpectedDwxNotify
Recovery:
1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact My Oracle Support (MOS).

22310 - Received Unexpected DPR/DPA

Event Type: DIAM
Description: DPR or DPA message was received from the peer when it was not expected.
Severity: Info
Instance: TransConnName
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterReceivedUnexpectedDpxNotify
Recovery:
1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**22311 - Invalid Diameter message received**

Event Type: DIAM
Description: Diameter message received from peer which was decodable but contained a semantic error.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterReceivedInvalidDiameterMessageNotify
Recovery:
1. Analyze MsgOctets to determine which semantic error occurred and diagnose peer for unexpected behavior.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**22312 - Socket send failure**

Event Type: DIAM
Description: An unexpected error occurred during the socket send call when attempting to send a Diameter message to the peer.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterFailedToSendDiameterMessageNotify
Recovery:
1. Analyze error value to determine root cause.
2. If the problem persists, contact *My Oracle Support (MOS)*.
22313 - Connection Unavailable: Transport failure

Event Type: DIAM
Description: The connection was closed by the SCTP or TCP transport.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailTransportFailureNotify
Recovery:
1. Analyze error value to determine root cause.
2. If the problem persists, contact My Oracle Support (MOS).

22314 - Connection Unavailable: CEA Realm/Host validation failure

Event Type: DIAM
Description: Origin-Realm and/or Origin-Host in CEA message received from peer on locally initiated connection does not match the locally configured connection.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailCeaRealmHostVldtnFailNotify
Recovery:
1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration using the Diameter > Configuration > Local Nodes page.
2. If the problem persists, contact My Oracle Support (MOS).

22315 - Connection Unavailable: Peer IP address validation failure

Event Type: DIAM
Description: Actual peer connection IP address does not match configured peer IP address.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailPeerIpAddrVldtnFailNotify

Recovery:
1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration using the Diameter > Configuration > Local Nodes page.
2. If the problem persists, contact My Oracle Support (MOS).

22316 - Connection Unavailable: No common apps

Event Type: DIAM
Description: No common applications were found between local node and peer node during capabilities exchange.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailNoCommonAppsNotify

Recovery:
1. Reconcile Application IDs between local and peer nodes. If no common applications exist, the connection should be deleted or Disabled.
2. If the problem persists, contact My Oracle Support (MOS).

22317 - Connection Rejected: Connection already established

Event Type: DIAM
Description: Peer initiated connection was rejected because locally initiated connection has already completed capabilities exchange.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterConnRejectedConnAlrdyEstdNotify

Recovery:
1. If condition persists, diagnose peer to determine reason for the second connection initiation.
2. If the problem persists, contact My Oracle Support (MOS).

22318 - Connection Rejected: Connection not Enabled

Event Type: DIAM
**Description:** Peer initiated connection was rejected because connection was locally Admin Disabled.

**Severity:** Info

**Instance:** <TransConnName>

**HA Score:** Normal

**Throttle Seconds:** 30

**OID:** eagleXgDiameterConnRejectedConnNotEnabledNotify

**Recovery:**
1. Resolve inconsistency between the local and peer nodes Administrative State.
2. If the problem persists, contact *My Oracle Support (MOS)*.

---

**22319 - Connection Unavailable: Diameter Watchdog**

**Event Type:** DIAM

**Description:** Connection closed due to no traffic from peer within Tw*2 time after sending DWR.

**Severity:** Info

**Instance:** <TransConnName>

**HA Score:** Normal

**Throttle Seconds:** 1

**OID:** eagleXgDiameterConnUnavailWatchdogFailureNotify

**Recovery:**
1. Confirm that the connection is not administratively Disabled at the peer.
2. Confirm that the peer connection configuration (protocol, remote/local IP address, remote/local port) matches local connection configuration.
3. Confirm there is reliable IP network connectivity between the peer IP and the local IP for the connection (no excess packet loss).
4. 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.
5. If the problem persists, contact *My Oracle Support (MOS)*.

---

**22320 - Invalid peer initiated connection**

**Event Type:** DIAM

**Description:** Origin-Realm and or Origin-Host in CER message received or the peer IP addresses advertised on peer initiated connection does not match any locally configured connection

**Severity:** Info

**Instance:** <MPName>

**HA Score:** Normal

**Throttle Seconds:** 30
OID: eagleXgDiameterInvalidPeerInitdConnNotify

Recovery:
1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration.
2. If the problem persists, contact My Oracle Support (MOS).

22321 - Connection Unavailable: DNS Resolution Failure

Event Type: DIAM
Description: During connection initiation, Transport/Peer FQDN was unable to be resolved to an IP address via DNS
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailDnsResolutionFailureNotify

Recovery:
1. Confirm DNS is available and reachable by MP.
2. Confirm that DNS configuration contains peer FQDN and appropriate corresponding IP address(es).
3. Analyze errno value and text from Event Addn’1 Info to determine root cause.
4. If the problem persists, contact My Oracle Support (MOS).

22322 - Connection Proving Success

Event Type: DIAM
Description: The connection proving phase completed successfully.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnProvingSuccessNotify

Recovery:
No action required.

22324 - Connection Unavailable: CER validation failure

Event Type: DIAM
Description: CER contained invalid or unsupported AVP or AVP value.
Severity: Info  
Instance: <TransConnName>  
HA Score: Normal  
Throttle Seconds: 1  
OID: eagleXgDiameterConnUnavailCerValidationFailureNotify  
Recovery:  
1. Disable peer’s use of inband security.  
2. If the problem persists, contact *My Oracle Support (MOS)*.

**22325 - Host-IP-Address AVP(s) in CER/CEA do not match peer IP address(es)**

Event Type: DIAM  
Description: The Host-IP-Address AVP(s) received in a CER or CEA message from the peer did not match the actual peer connection’s IP address(es).  
Severity: Info  
Instance: <TransConnName>  
HA Score: Normal  
Throttle Seconds: 1  
OID: eagleXgDiameterConnUnavailCerHostIpAvpVldtnFailNotify  
Recovery:  
1. Diagnose peer to resolve inconsistency.  
2. If the problem persists, contact *My Oracle Support (MOS)*.

**22326 - Connection Established**

Event Type: DIAM  
Description: The peer connection is available for signaling traffic.  
Severity: Info  
Instance: <TransConnName>  
HA Score: Normal  
Throttle Seconds: 1  
OID: eagleXgDiameterConnEstablishedNotify  
Recovery:  
No action required.
22327 - Initiator function disabled

**Event Type:** DIAM

**Description:** Peer disconnect reason indicated that we should not attempt to initiate a connection.

**Severity:** Info

**Instance:** <TransConnName>

**HA Score:** Normal

**Throttle Seconds:** 1

**OID:** eagleXgDiameterInitiatorFunctionDisabledNotify

**Recovery:**
1. No action required. The peer can still initiate a connection. If the peer does not attempt to initiate a connection within a reasonable amount of time, the connection can be disabled, then re-enabled to re-activate the initiator function.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22328 - Connection is processing a higher than normal ingress messaging rate

**Alarm Group:** DIAM

**Description:** The diameter connection specified in the alarm instance is processing a higher than normal ingress messaging rate.

**Severity:**
- Minor (if all of the following are true):
  - The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection minor alarm threshold.
  - The average ingress MPS rate that the connection is processing has not yet reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.
- Major (if 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:** The name of the diameter connection as defined by the TransportConnection table.

**HA Score:** Normal

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

**OID:** eagleXgDiameterIngressMpsRateNotify

**Recovery:**
1. The Diameter connection specified in the Alarm Instance field is processing a higher than expected average ingress Diameter message rate. The alarm thresholds for minor and major alarms are configured in the Capacity Configuration Set used by the Diameter connection.
2. The message rate used for this alarm is an exponentially smoothed 30 second average. This smoothing limits false alarms due to short duration spikes in the ingress message rate.

3. If the alarm severity is minor, the alarm means 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.

**22329 - SCTP Connection Impaired: A path has become unreachable**

- **Event Type:** DIAM
- **Description:** A path of an established SCTP connection has become unreachable.
- **Severity:** Info
- **Instance:** <TransConnName:Peer IP> (peer/remote IP of the failed path)
- **HA Score:** Normal
- **Throttle Seconds:** 10
- **OID:** eagleXgDiameterSctpConnectionImpairedNotify
- **Recovery:**
  1. Check whether the routing path between the local IP address and the peer IP address is up. If it is not, fix it.
  2. If the problem persists, contact *My Oracle Support (MOS)*.

**22330 - SCTP Connection Cfg Mismatch: The peer advertised a different number of IP addresses than configured**

- **Event Type:** DIAM
- **Description:** The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.
- **Severity:** Info
- **Instance:** <TransConnName>
- **HA Score:** Normal
- **Throttle Seconds:** 1
- **OID:** eagleXgDiameterSctpConnectionCfgMismatchNotify
- **Recovery:**
Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the Diameter > Configuration > System Options page.

22331 - SCTP Connection Partial Matching: SCTP connection accepted but the IP addresses advertised by the peer match only partially those configured for the peer in the connection object

Event Type: DIAM
Description: The peer has advertised in the INIT/INIT_ACK chunk a set of IP addresses which overlap but does not include all the IP addresses configured for the peer in the respective connection object.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterSCTPConnectionPartialMatchingNotify
Recovery:
1. Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the Diameter > Configuration > System Options page.
2. If the problem persists, contact My Oracle Support (MOS).

22332 - Connection Rejected: Max Connections Exceeded

Event Type: DIAM
Description: Connection was rejected due to the DA-MP exceeding its maximum number of supported Diameter Connections.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnRejMaxConnExceededNotify
Recovery:
1. If the DA-MP is a member of a IPFE TS, verify that the IPFE is configured to fully monitor the DA-MP’s availability status.
When a IPFE fully monitors application servers in a IPFE TS, it will cease from distributing new Diameter connections to any/all application servers that report a “Stasis” availability status.
2. If the problem persists, contact My Oracle Support (MOS).
22333 - Connection Rejected: Insufficient Ingress MPS

Event Type: DIAM

Description: Connection was rejected due to insufficient Ingress MPS on the DA-MP to support the Reserved Ingress MPS configured for the connection. This sum of the Reserved Ingress MPS for the added connection and MP Reserved Ingress MPS has exceeded the MP Maximum Reserved Ingress MPS.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterConnRejInsufficientIngressMpsNotify

Recovery:
1. The value for Reserved Ingress MPS for the added connection needs to be examined to determine if its value should be decreased.
2. Contact My Oracle Support (MOS) for assistance.

22334 - Unexpected Message Priority in ingress Request

Event Type: DIAM

Description: The decoded Message Priority from the ingress Request has an unexpected value.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterUnexpMessagePriorityInRequestNotify

Recovery:
1. Verify that the peer is a DSR
   - Product-Name is reported as “Eagle XG DSR”, in the Event Additional Information.
   - Vendor-Id is reported as 323 (Tekelec).
2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.
   - Call My Oracle Support (MOS) and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   - If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call My Oracle Support (MOS).
   - If the reported Firmware-Version is less than the minimum required DSR software version, call My Oracle Support (MOS) to seek advice on whether the peer DSR needs to be upgraded, or
whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to “None”.

22335 - Peer does not support Message Priority

Event Type: DIAM
Description: Cannot read Message Priority from ingress Requests because Peer does not support Message Priority.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 20
OID: eagleXgDiameterMessagePriorityNotSuppPeerNotify
Recovery:
1. Verify that the peer is a DSR
   • Product-Name is reported as “Eagle XG DSR”, in the Event Additional Information.
   • Vendor-Id is reported as 323 (Tekelec).
2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.
   • Call My Oracle Support (MOS) and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   • If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call My Oracle Support (MOS).
   • If the reported Firmware-Version is less than the minimum required DSR software version, call My Oracle Support (MOS) to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to “None”.

22336 - Connection Rejected: Multihomed SCTP connection attempt

Event Type: DIAM
Description: Connection was rejected because the peer attempted to initiate an SCTP multihomed connection to an IPFE connection.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterConnRejMHSctpConnAttemptNotify
Recovery:
1. Update the peer to initiate unihomed IPFE SCTP connections.
2. Contact the *My Oracle Support (MOS)* for assistance.

22343 - Connection Unavailable: Duplicate Connection Released

**Event Type:** DIAM  
**Description:** Duplicate connection established, connection terminated.  
**Severity:** Info  
**Instance:** <TransConnName>  
**HA Score:** Normal  
**Throttle Seconds:** 1  
**OID:** eagleXgDiameterDuplicateConnectionReleasedNotify  
**Recovery:**  
No action necessary.

22344 - Failed to process ingress message: Processor Unavailable or Congested

**Event Type:** DIAM  
**Description:** The message processor is Unavailable or Congested. This event refers to another DA-MP, not the one reporting the problem.  
**Severity:** Info  
**Instance:** <SourceMpHost>  
**HA Score:** Normal  
**Throttle Seconds:** 10  
**OID:** eagleXgDiameterProcessorUnavlblOrCngstedNotify  
**Recovery:**  
Contact *My Oracle Support (MOS)* for further assistance.

22345 - Connection Priority Level changed

**Event Type:** DIAM  
**Description:** The Diameter Connection’s CPL has transitioned from its current value to a new CPL value based on congestion levels reported by various features.  
**Severity:** Info  
**Instance:** <TransConnName>  
**HA Score:** Normal  
**Throttle Seconds:** 0 (zero)
OID: eagleXgDiameterCplChangedNotify

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. Identify the most recent “Connection Degraded” event in the event log for the connection and utilize the Event Detailed information to diagnose the condition.
3. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

22346 - MP Reserved Ingress MPS Oversubscribed

**Event Type:** DIAM  
**Description:** The total connection Reserved Ingress MPS exceeds the Engineered Ingress MPS capacity of the MP.  
**Severity:** Info  
**Instance:** MPName (Hostname of the DA-MP Server)  
**HA Score:** Normal  
**Throttle Seconds:** 1  

**OID:** eagleXgDiameterMpResIngressMpsOversubscribedNotify

**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. Perform one or more of these actions:
   - Increase the maximum reserved capacity by increasing the value of IPFE Connection Reserved Ingress MPS Scaling parameter.
   - Reduce the subscribed amount of reserved capacity by reducing the number of connections.
   - Reduce the reserved capacity required by connections.
3. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

22347 - Ingress Message Discarded: DA-MP shared ingress capacity exhausted

**Alarm Type:** DIAM  
**Description:** An ingress message is discarded on a DA-MP due to the ingress message rate on the DA-MP exceeding MP Maximum Ingress MPS.  
**Severity:** N/A  
**Instance:** <MPHostName>  
**HA Score:** Normal  
**Throttle Seconds:** 30
OID: eagleXgDiameterMpIngressMessageDiscardedNotify

Recovery:
1. The ingress MPS on the DA-MP is exceeding the MP Maximum Ingress MPS. Consider decreasing the overall ingress message rate on the DA-MP by diverting the traffic or reducing the traffic.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.

22349 - IPFE Connection Alarm Aggregation Threshold

Alarm Type: 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: Critical, Major

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. Contact My Oracle Support (MOS) for assistance.

22350 - Fixed Connection Alarm Aggregation Threshold

Alarm Type: 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: Critical, Major

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. Contact My Oracle Support (MOS) for assistance.

22900 - DPI DB Table Monitoring Overrun
Event Type: DIAM
Description: The COMCOL update sync log used by DB Table monitoring to synchronize Diameter Connection Status among all DA-MP RT-DBs has overrun. The DA-MP’s Diameter Connection Status sharing table is automatically audited and re-synced to correct any inconsistencies.
Severity: Info
Instance: <DbTblName>
Note: <DbTblName> refers to the name of the Diameter Connection Status Sharing Table the Diameter Connection status inconsistency that was detected.
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterDpiTblMonCbOnLogOverrunNotify
Recovery:
Contact My Oracle Support (MOS) if this alarm is constantly being asserted and cleared.

22901 - DPI DB Table Monitoring Error
Event Type: DIAM
Description: An unexpected error occurred during DB Table Monitoring.
Severity: Info
Instance: DpiTblMonThreadName
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterDpiSldbMonAbnormalErrorNotify
Recovery:
22950 - Connection Status Inconsistency Exists

Alarm Type: DIAM
Description: Diameter Connection status inconsistencies exist among the DA-MPs in the DSR signaling NE.
Severity: Critical
Instance: <MpName> (where inconsistency detected)
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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

Alarm Type: DIAM
Description: A DA-MP configuration profile has not been assigned to this DA-MP.
Severity: Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDaMpProfileNotAssignedNotify
Recovery:

  1. A DA-MP profile must be assigned to the DA-MP via the DSR OAM GUI.
  2. If the problem persists, contact My Oracle Support (MOS).

22961 - Insufficient Memory for Feature Set

Alarm Type: DIAM
Description: The Available Memory (in kilobytes) for Feature Set is less than the Required Memory (in kilobytes).
Severity: Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterInsufficientAvailMemNotify
Recovery:
1. Make additional memory available on the DA-MP for the configured DiameterMaxMessageSize.
2. If the problem persists, contact My Oracle Support (MOS).

Range Based Address Resolution (RBAR) Alarms and Events (22400-22424)

22400 - Message Decoding Failure

Event Type: RBAR
Description: A message received was rejected because of a decoding failure.
Severity: Info
Instance: <MPName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterRbarMsgRejectedDecodingFailureNotify
Recovery:

While parsing the message, the message content was inconsistent with the Message Length in the
message header. These protocol violations can be caused by the originator of the message (identified
by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

22401 - Unknown Application ID

Event Type: RBAR
Description: A message could not be routed because the Diameter Application ID is not supported.
Severity: Info
Instance: <MPName>
HA Score: Normal
Throttle Seconds: 10
OID: 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.

22402 - Unknown Command Code

Event Type: RBAR
Description: A message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.
Severity: Info
Instance: <MPName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterRbarUnknownCmdCodeNotify
Recovery:
1. The order pair (Application ID, Command Code) is not provisioned in the Address Resolutions routing configuration.
2. View the currently provisioned Application IDs and Command Codes by selecting RBAR > Configuration > Address Resolutions.

22403 - No Routing Entity Address AVPs

Event Type: RBAR
Description: A message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.
Severity: Info
Instance: <AddressResolution>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterRbarNoRoutingEntityAddrAvpNotify
Recovery:
1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting RBAR > Configuration > Address Resolutions.
22404 - No valid Routing Entity Addresses found

Event Type: RBAR

Description: A message could not be routed because none of the address AVPs contained a valid address and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarNoValidRoutingEntityAddrFoundNotify

Recovery:
1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting RBAR > Configuration > Address Resolutions.

22405 - Valid address received didn’t match a provisioned address or address range

Event Type: RBAR

Description: A message could not be routed because a valid address was found that did not match an individual address or address range associated with the Application ID, Command Code, and Routing Entity Type, and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarAddrMismatchWithProvisionedAddressNotify

Recovery:
1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting RBAR > Configuration > Address Resolutions.

22406 - Routing attempt failed due to internal resource exhaustion

Event Type: RBAR
**Description:** A message could not be routed because the internal "Request Message Queue" to the DSR Relay Agent was full. This should not occur unless the MP is experiencing local congestion as indicated by Alarm-ID **22200 - Local MP Congestion**.

**Severity:** Info

**Instance:** <MPName>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterRbarRoutingAttemptFailureInternalResExhNotify

**Recovery:**

If this problem occurs, contact *My Oracle Support (MOS)*.

---

**22407 - Routing attempt failed due to internal database inconsistency failure**

**Event Type:** RBAR

**Description:** A message could not be routed because an internal address resolution run-time database inconsistency was encountered.

**Severity:** Info

**Instance:** <MPName>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterRbarRoutingFailureInternalDbInconsistencyNotify

**Recovery:**

If this problem occurs, 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**

**Alarm Type:** APPL

**Description:** DSR Application is unable to process any messages because it is Unavailable

**Severity:** Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationUnavailableNotify

Recovery:
1. Display and monitor the DSR Application status by 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 DSR Application can also become Unavailable when it reaches Congestion Level 3 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.
4. Check the Event History logs for additional DIAM events or alarms for this MP server.
5. If the problem persists, contact My Oracle Support (MOS).

22501 - DSR Application Degraded

Alarm Type: APPL

Description: Unable to forward requests to the DSR Application because it is Degraded

Severity: Major

Instance: <DSR Application Name>

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationDegradedNotify

Recovery:
1. Display and monitor the DSR Application status by 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, contact My Oracle Support (MOS).
22502 - DSR Application Request Message Queue Utilization

**Alarm Type:** APPL

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

**Severity:**
- **Minor:** Request Queue utilization becomes over 60%
- **Major:** Request Queue utilization becomes over 80%
- **Critical:** Request Queue utilization becomes over 95%

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

**Note:** The value for Metric ID for this alarm will vary (RxPdraRequestMsgQueue, RxCpaRequestMsgQueue for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

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

**HA Score:** Normal

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

**OID:** 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 Routing Rules**.

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, contact **My Oracle Support (MOS)**.

---

22503 - DSR Application Answer Message Queue Utilization

**Alarm Type:** APPL

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

**Severity:**
- **Minor:** Answer Queue utilization becomes over 60%
- **Major:** Answer Queue utilization becomes over 80%
- **Critical:** Answer Queue utilization becomes over 95%
Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraAnswerMsgQueue, RxCpaAnswerMsgQueue for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

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

HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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 Routing Rules 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, contact My Oracle Support (MOS).

22504 - DSR Application Ingress Message Rate

Alarm Type: APPL

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

Severity:
• Minor: Ingress Message Rate becomes over 110% of the ingress message capacity
• Major: Ingress Message Rate becomes over 140% of the ingress message capacity
• Critical: Ingress Message Rate becomes over 160% of the ingress message capacity

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

Note: 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.

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

HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDsrApplicationIngressMsgRateNotify
Recovery:
1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting Diameter > Configuration > Application Routing Rules 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, contact My Oracle Support (MOS).

25510 - Multiple DA-MP Leader Detected Alarm

Alarm Type: DIAM
Description: This alarm occurs when multiple active DA-MP leaders have been detected.
Severity: Critical
Instance: <NetworkElement>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMultipleDaMpLeadersDetectedNotify
Recovery: If the problem persists, contact My Oracle Support (MOS) for assistance.

22520 - DSR Application Enabled

Event Type: APPL
Description: DSR Application Admin state was changed to ‘enabled’.
Severity: Info
Instance: <DSR Application Name>
HA Score: Normal
Throttle Seconds: 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>
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:**

Contact *My Oracle Support (MOS)* for assistance.

22601 - Unknown Application ID

**Event Type:** FABR

**Description:** Message could not be routed because the Diameter Application ID is not supported.

**Severity:** Info

**Instance:** <MPName>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterFabrUnknownAppIdNotify

**Recovery:**
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.

1. The currently provisioned Application Routing Rules can be viewed using Main Menu > Diameter > Configuration > Application Routing Rules.
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

Event Type: FABR
Description: Message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.
Severity: Info
Instance: <MPName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterFabrUnknownCmdCodeNotify
Recovery:
Either an application routing rule is mis-provisioned or the Command Code is not provisioned in the FABR configuration.
1. The currently provisioned Application Routing Rules can be viewed using Main Menu > Diameter > Configuration > Application Routing Rules.
2. The currently provisioned Diameter Application IDs can be viewed in the FABR > Configuration > Address Resolutions.
3. Contact My Oracle Support (MOS) for assistance.

22603 - No Routing Entity Address AVPs

Event Type: FABR
Description: Message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.
Severity: Info
Instance: <AddrResolution>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterFabrNoRoutingEntityAddrAvpNotify
Recovery:
1. If this event is considered abnormal, then validate which AVPs are configured for routing with the Application ID and Command Code using **FABR > Configuration > Address Resolutions**.

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

3. Contact **My Oracle Support (MOS)** for assistance.

---

**22604 - No valid User Identity Addresses found**

- **Event Type:** FABR
- **Description:** No valid User Identity Address is found in the configured AVPs contained in the ingress message.
- **Severity:** Info
- **Instance:** <AddrResolution>
- **HA Score:** Normal
- **Throttle Seconds:** 10
- **OID:** 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 Routing Rules**.

3. Contact **My Oracle Support (MOS)** for assistance.

---

**22605 - No Destination address is found to match the valid User Identity address**

- **Event Type:** FABR
- **Description:** Message could not be routed because the valid user identity address extracted from the message did not resolve to a destination address. The Routing Exception was configured to send an Answer response. Please verify the provisioning in the address resolution table and the data provided in the SDS corresponding to this address/resolution entry.
- **Severity:** Info
- **Instance:** <AddrResolution>
- **HA Score:** Normal
- **Throttle Seconds:** 10
- **OID:** eagleXgDiameterFabrNoAddrFoundAtDpNotify

**Recovery:**

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.

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. 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:
   Contact My Oracle Support (MOS) for assistance.

22607 - Routing attempt failed due to DRL queue exhaustion

Event Type: FABR
Description: Message could not be routed because the internal “Request Message Queue” to the DSR Relay Agent was full.
Severity: Info
Instance: <MPNname>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterFabrRoutingAttemptFailureDrlQueueExhNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance.

22608 - Database query could not be sent due to DB congestion

Event Type: FABR
Description: FABR could not send a database query either because the ComAgent reported DP congestion level of (CL=2 or 3), or an abatement period is in progress.
Severity: Info
Instance: <MPNname>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterFabrDpCongestedNotify
Recovery:
Contact My Oracle Support (MOS) for assistance.

22609 - Database connection exhausted

Event Type: FABR
Description: Database queries could not be sent because the database connection (ComAgent) queue was full
Severity: Info
Instance: <MPNname>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterFabrDbConnectionExhNotify
Recovery:
Contact My Oracle Support (MOS) for assistance.

22610 - FABR DP Service congestion state change

Event Type: FABR
Description: FABR application received status notification indicating DP congestion state change or DP congestion abatement time period has completed.
Severity: Info
Instance: <MPName>
HA Score: Normal
Throttle Seconds: 0 (zero)
OID: eagleXgDiameterFabrDpCongestionStateChangeNotify
Recovery:
Contact My Oracle Support (MOS) for assistance.

22611 - FABR Blacklisted Subscriber

Event Type: FABR
Description: Message could not be routed because valid User Identity Address extracted from diameter request belongs to blacklisted subscriber.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrBlacklistedSubscriberNotify

Recovery:
The destination address associated with User Identity address derived is blacklisted in the address mapping configuration on DDR.
1. Validate which User identity address is not blacklisted by using DP configuration.
2. If the problem persists, contact My Oracle Support (MOS).

22631 - FABR DP Response Task Message Queue Utilization

Alarm Type: FABR

Description: The FABR Application’s DP Response Message Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxFabrDpResponseMsgQueue, FABR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterFabrAppDpResponseMessageQueueUtilizationNotify

Recovery:
1. This alarm may occur due to persistent overload conditions with respect to database response processing.
2. Contact My Oracle Support (MOS) for assistance.

22632 - COM Agent Registration Failure

Alarm Type: 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
Policy DRA (PDRA) Alarms and Events (22700-22799)

22700 - Protocol errors in Diameter Requests

Event Group: PDRA
Description: The Diameter request message(s) received by Policy DRA contain protocol error(s).
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: pdraPdraProtocolErrorsInDiameterReqNotify
Recovery:
    Contact My Oracle Support (MOS) for assistance.

22701 - Protocol errors in Diameter Answers

Event Group: PDRA
Description: The Diameter answer message(s) received by Policy DRA contain(s) protocol error(s). The Error Message is based on the specific error scenario.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: pdraPdraProtocolErrorsInDiameterAnsNotify
Recovery:
    Contact My Oracle Support (MOS) for assistance.

22702 - Database Hash Function Error

Event Type: PDRA
Description: The hash function result does not map to a database resource or sub-resource
Severity: Info
22703 - Diameter message routing failure due to DRL queue exhaustion

Event Type: PDRA
Description: The Diameter egress message (request or answer) could not be sent due to DRL queue exhaustion.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: pdraPdraEgressMsgRoutingFailureDueToDrlQueueExhaustedNotify
Recovery: 
Contact My Oracle Support (MOS) for assistance.

22704 - Policy DRA Communication Agent Error

Event Type: PDRA
Description: A communication failure occurs between the Policy DRA server and the Policy SBR server.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: pdraPdraStackEventSendingFailureCAUnavailNotify
Recovery: 
Contact My Oracle Support (MOS) for assistance.

22705 - Policy SBR Error Response Received By Policy DRA

Event Type: PDRA
Description: The Policy DRA server received a response from the Policy SBR server indicating Policy SBR errors.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: pdraPdraPsbrErrorIndicationNotify
Recovery:
    Contact *My Oracle Support (MOS)* for assistance.

### 22706 - Binding Key Not Found In Diameter Message

**Event Type:** PDRA  
**Description:** A binding key is not found in the received CCR-I message.  
**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Throttle Seconds:** 60  
**OID:** pdraPdraBindingKeyNotFoundNotify  
**Recovery:**  
1. Check the P-DRA GUI at *Policy DRA > Configuration > Binding Key Priority.*  
2. Contact *My Oracle Support (MOS)* for assistance.

### 22707 - Policy DRA Diameter Message Processing Failure

**Alarm Type:** PDRA  
**Description:** The Policy DRA failed to process a Diameter message. The specific reason is provided by the Policy DRA signaling code.  
**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Throttle Seconds:** 60  
**OID:** pdraPdraDiameterMessageProcessingFailureNotify  
**Recovery:**  
    Contact *My Oracle Support (MOS)* for further assistance.

### 22710 - Policy SBR Sessions Threshold Exceeded

**Alarm Type:** pSBR
Description: The number of sessions threshold for a Policy DRA Mated Sites Place Association has been exceeded.

Severity:
- **Minor**: pSBR session numbers are greater than or equal to 80% of maximum session capacity
- **Major**: pSBR session numbers are greater than or equal to 90% of maximum session capacity
- **Critical**: pSBR session numbers are greater than or equal to 95% of maximum session capacity

Instance: Policy DRA Mated Sites Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrActSessThreshNotify

Recovery:
1. Determine if the alarm thresholds for Session Capacity are properly configured on the PDRA Network OAM GUI Main Menu from **Policy DRA > Configuration > Alarm Settings**. 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, contact [My Oracle Support (MOS)](https://www.oracle.com) for further assistance.

**22711 - Policy SBR Database Error**

Alarm Type: pSBR

Description: An error occurred during a Policy SBR database operation.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterPSBRDbOpFailNotify

Recovery:

Contact [My Oracle Support (MOS)](https://www.oracle.com) for further assistance.

**22712 - Policy SBR Communication Error**

Alarm Type: pSBR

Description: The Policy SBR received an error or timeout response from Communication Agent.

Severity: Info
22713 - Policy SBR Alternate Key Creation Error

Alarm Type: pSBR
Description: An attempt to create an Alternate Key record in the Binding database failed.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterPSBRAltKeyCreateFailNotify
Recovery:
    Contact My Oracle Support (MOS) for further assistance.

22714 - Policy SBR RAR Initiation Error

Alarm Type: pSBR
Description: Policy SBR encountered an error while processing Policy DRA initiated RAR requests.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterPSBRRARInitiationErrNotify
Recovery:
    Contact My Oracle Support (MOS) for further assistance.

22715 - Policy SBR Audit Suspended

Alarm Type: pSBR
Description: This alarm indicates that Policy SBR binding and / or session auditing has been suspended due to a congestion condition on either the local server reporting the alarm, or on a remote server being queried for auditing purposes.
Severity: Minor
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterPSBRAuditSuspendedNotify

Recovery:
1. The Policy SBR 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 Policy SBR server. Investigate the causes of congestion on the Policy SBR servers (see also Alarm 22725 - Policy SBR Server In Congestion).
2. If the problem persists, contact My Oracle Support (MOS).

22716 - Policy SBR Audit Statistics Report

Event Group: pSBR

Description: This report provides statistics related to Policy SBR session or binding table audits. Each Policy SBR server generates this event upon reaching the last record in a table. The statistics reported are appropriate for the type of table being audited. This report also provides hourly statistics related to the Pending RAR report.

Severity: Info
Instance: None
HA Score: Normal
Throttle Seconds: 0 (no throttling)
OID: eagleXgDiameterPSBRAuditStatisticsReportNotify

Recovery:
Contact My Oracle Support (MOS).

22717 - Policy SBR Alternate Key Creation Failure Rate

Alarm Type: pSBR

Description: Policy SBR Alternate Key Creation Failure rate exceeds threshold.
Severity: Minor, Major, Critical
Instance: PDRA Mated Pair Place Association
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterPSBRAltKeyCreationFailureRateNotify

Recovery:
1. Check ComAgent Congestion alarms on the Binding PSBRs. If the Binding PSBRs are congested, it is likely that there is a very high rate of Diameter traffic.

2. Check the ComAgent connections statuses. This issue can occur if the ComAgent connections between the Session and Binding PSBRs are not "In Service". ComAgent connection statuses can be found on the Active NOAMP GUI at Main Menu > Communication Agent > Maintenance > Connection Status.

3. If any of the connections are disabled, change the administrative state to enabled. If any connections are enabled but not "In Service", there could be a network issue.

4. If the further assistance is needed, contact My Oracle Support (MOS).

**22718 - Binding Not Found for Binding Dependent Session Initiate Request**

- **Event Group:** PDRA
- **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 PDRA GUI Main Menu Policy DRA > 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:** pSBR
- **Description:** The maximum number of sessions per binding is exceeded that fails the attempt to create a binding for a given subscriber key
- **Severity:** Info
- **Instance:** N/A
- **HA Score:** Normal
- **Throttle Seconds:** 60
- **OID:** pdraPdraMaxSessionsReachedNotify

**Recovery:**
1. Determine if the existing sessions are valid. The existing sessions may be displayed using the Binding Key Query Tool to obtain all relevant information including session-ids and PCEF FQDNs.
2. If the sessions exist in the P-DRA but not on the PCEF(s), call the My Oracle Support (MOS).
22720 - Policy SBR To Policy DRA Response Queue Utilization Threshold Exceeded

**Alarm Type:** PDRA

**Description:** The Policy DRA's pSBR Response Queue threshold has been exceeded.

**Severity:**
- **Minor:** pSBR Response Queue Utilization becomes over 60%
- **Major:** pSBR Response Queue Utilization becomes over 80%
- **Critical:** pSBR Response Queue Utilization becomes over 95%

**Instance:** RxPdraSbrEventMsgQueue, Policy DRA

**HA Score:** Normal

**OID:** pdraPdraPsbrResponseQueueUtilizationNotify

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

**Recovery:**
1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from 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, contact My Oracle Support (MOS).

22721 - Policy DRA Server In Congestion

**Alarm Type:** PDRA

**Description:** The operational state of the Policy DRA is congested.

**Severity:**
- **Minor:** ingress Request rate is 110% of PR-MPS or larger
- **Major:** ingress Request rate is 140% of PR-MPS or larger
- **Critical:** ingress Request rate is 160% of PR-MPS or larger

**Instance:** Policy DRA

**HA Score:** Normal

**OID:** pdraPdraCongestionStateNotify

**Auto Clear Seconds:** 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 Routing Rules.

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, contact My Oracle Support (MOS).

22722 - Policy DRA Binding Sub-resource Unavailable

Alarm Type: PDRA
Description: One or more of the binding sub-resources are not available.
Severity:
- **Major**: When at least one of the binding sub-resources is not available
- **Critical**: When all of the binding sub-resources is not available
Instance: Policy DRA
HA Score: Normal
OID: pdraPdraBindingSubresourceUnavailableNotify
Auto Clear Seconds: 0 (zero)
Recovery:
1. Monitor the P-DRA Binding Resource on the P-DRA Network OAM at Main Menu > Configuration > Resource Domains
2. If the problem persists, contact My Oracle Support (MOS).

22723 - Policy DRA Session Sub-resource Unavailable

Alarm Type: PDRA
Description: One or more of the session sub-resources are not available.
Severity:
- **Major**: When at least one of the server groups hosting session sub-resources is not available
- **Critical**: When all of the server groups hosting session sub-resources are not available
Instance: Policy DRA
HA Score: Normal
OID: pdraPdraSessionSubresourceUnavailableNotify
Auto Clear Seconds: 0 (zero)
Recovery:
1. Monitor the P-DRA Session Resource at Main Menu > Configuration > Resource Domains
2. If the problem persists, contact My Oracle Support (MOS).
22724 - Policy SBR Memory Utilization Threshold Exceeded

Alarm Type: pSBR

Description: The Policy SBR server memory utilization threshold has been exceeded.

Severity:
- **Minor**: pSBR memory utilization threshold exceeds 70%
- **Major**: pSBR memory utilization threshold exceeds 80%
- **Critical**: pSBR memory utilization threshold exceeds 90%

Instance: Policy DRA Mated Sites Place Association

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrMemUtilNotify

Recovery:
1. If this condition persists, it may be necessary to allocate more memory for pSBR.
2. Contact *My Oracle Support (MOS)* for further assistance.

22725 - Policy SBR Server In Congestion

Alarm Type: pSBR

Description: The Policy SBR server is operating in congestion.

Severity:
- **Minor**: CL_1
- **Major**: CL_2
- **Critical**: CL_3

Instance: None

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrServerInCongestionNotify

Recovery:
1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting *Diameter > Configuration > Application Routing Rules*.
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, contact *My Oracle Support (MOS)*.
22726 - Policy SBR Queue Utilization Threshold Exceeded

Alarm Type: pSBR

Description: The Policy SBR queue utilization has reached the configured threshold values.

Severity:
- **Minor**: pSBR stack event queue utilization threshold exceeds 60%
- **Major**: pSBR stack event queue utilization threshold exceeds 80%
- **Critical**: pSBR stack event queue utilization threshold exceeds 95%

Instance: Policy DRA Mated Sites Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrStackEvQUtilNotify

Recovery:
1. If this condition persists, it may be necessary to allocate larger queue sizes.
2. Contact *My Oracle Support (MOS)* for further assistance.

22727 - Policy SBR Initialization Failure

Alarm Type: pSBR

Description: The Policy SBR server psbr process failed to initialize.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrInitializationFailureNotify

Recovery:
Contact *My Oracle Support (MOS)* for further assistance.

22728 - Policy SBR Bindings Threshold Exceeded

Alarm Type: pSBR

Description: The number of Policy SBR bindings threshold has been exceeded.

Severity:
- **Minor**: pSBR active bindings threshold is greater than or equal to 80% of maximum binding capacity
- **Major**: pSBR active bindings threshold is greater than or equal to 90% of maximum binding capacity
- **Critical**: pSBR active bindings threshold is greater than or equal to 95% of maximum binding capacity
Instance: PDRA Binding Region Place Association
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterPSbrActBindThreshNotify
Recovery:
1. Determine if alarm thresholds for Binding Capacity are properly configured on the PDRA Network OAM GUI Main Menu from **Policy DRA > Configuration > Alarm Settings**. Alarm severity is determined by the number of binding records stored in the Binding Region exceeding the alarm threshold percentage of the calculated binding 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 1 binding per policy subscriber.
4. If the system is nearing 100% capacity, contact **My Oracle Support (MOS)** for further assistance.

22729 - PCRF Not Configured

Alarm Type: PDRA
Description: PCRFs connected to the Policy DRA are not configured.
Severity: Critical
Instance: Policy DRA
HA Score: Normal
OID: pdraPcrfNotConfiguredNotify
Auto Clear Seconds: 0 (zero)
Recovery:
1. Check the P-DRA GUI at **Main Menu > Policy DRA > Configuration > PCRFs** for further PCRF configuration.
2. Check the event history logs in **Alarms & Events**.
3. If the problem persists, contact **My Oracle Support (MOS)**.

22730 - Policy DRA Configuration Error

Alarm Group: PDRA
Description: Policy message processing could not be successfully completed due to a configuration error.
Severity: Major
Instance: "Unconfigured PCRF", "Unconfigured APN", "Missing APN", or "No Configured PCRFs"
HA Score: Normal
OID: pdraPdraConfigErrorNotify
Auto Clear Seconds: 300
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 DRA > Configuration > 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 DRA > Configuration > PCRFs. If the PCRF is not valid for the request, correct the routing table or tables that included the PCRF.

   See also RxBindCapUnknownPcrf.

2. If there is an unconfigured APN and if the APN string is valid, configure the APN at the NOAMP using the Policy DRA > 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.

   See also RxBindCapUnknownApn and RxBindDepUnknownApn.

3. If there is a missing APN, investigate the policy client to determine why it is sending policy session initiation requests with no APN.

   See also RxBindCapMissingApn and RxBindDepMissingApn.

4. If there are no PCRFs configured, configure PCRFs at the SOAM GUI for the site using Policy DRA > Configuration > PCRFs.

5. Contact My Oracle Support (MOS)

---

22731 - Policy DRA Database Inconsistency

**Alarm Type:** PDRA

**Description:** The Policy DRA Database data inconsistency exists due to an internal error such as table truncation, code error etc.

**Severity:** Major

**Instance:** Policy DRA

**HA Score:** Normal

**Auto Clear Seconds:** 60

**OID:** pdraPdraDbInconsistencyExistsNotify

**Recovery:**

1. Check the error history logs for the details of the data inconsistency.
2. If the problem persists, contact My Oracle Support (MOS).

---

22732 - Policy SBR Process CPU Utilization Threshold Exceeded

**Alarm Type:** pSBR

**Description:** The Policy SBR process on the indicated server is using higher than expected CPU resources.

**Severity:**

- **Minor:** pSBR process CPU utilization threshold exceeds 60%
• **Major**: pSBR process CPU utilization threshold exceeds 66%
• **Critical**: pSBR process CPU utilization threshold exceeds 72%

**Instance**: Policy DRA Mated Sites Place Association  
**HA Score**: Normal  
**Auto Clear Seconds**: 0 (zero)  
**OID**: eagleXgDiameterPSbrProcCpuThreshNotify  
**Recovery**:  
1. If this condition persists, it may be necessary to deploy more policy signaling capacity.  
2. Contact *My Oracle Support (MOS)* for further assistance.

**22733 - Policy SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration**  
**Alarm Group**: pSBR  
**Description**: The Policy SBR failed to free binding memory after PCRF Pooling binding migration.  
**Severity**: Minor  
**Instance**: None  
**HA Score**: Normal  
**Auto Clear Seconds**: 0  
**OID**: eagleXgDiameterPSBRPostMigrationMemFreeNotify  
**Recovery**:  
1. On systems upgraded from a release where Policy DRA was running, but that did not support PCRF Pooling, to a release that supports PCRF Pooling, binding data is migrated from the tables used by the old release to tables used by the new release. Once this migration process completes on a given binding policy SBR, a script is automatically executed to free memory for the old tables. If this script should fail for any reason to free the memory, this alarm is asserted.  
2. If additional assistance is needed, contact *My Oracle Support (MOS)*.

**22734 - Policy DRA Unexpected Stack Event Version**  
**Alarm Group**: PDRA  
**Description**: A server upgrade discovers an unexpected stack event library version because one of the following occurs:  
• An attempt is made to send a current version stack event, but the sender is informed that the target server only supports the old version.  
• An old version stack event is received after all servers should have been upgraded to support the new version  
**Severity**: Major  
**Instance**: None
HA Score: Normal
OID: pdraPdraUnexpectedSEDownVersionNotify
Auto Clear Seconds: 300

Recovery:
1. From the NOAMP GUI at Policy DRA > Maintenance > Policy 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 Policy 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, contact My Oracle Support (MOS).

22735 - Policy DRA session initiation request received with no APN

Event Group: PDRA
Description: A Policy DRA session initiation request was received with no APN.
Severity: Info
HA Score: Normal
Instance: None
Throttle Seconds: 30
OID: pdraPdraSessInitReqWithNoApnNotify

Recovery:
1. Investigate why the policy client named by the Origin-Host FQDN in the additional information field is not including the Called-Station-Id AVP and correct it to include the APN.
2. Investigate why the policy client named by the Origin-Host FQDN in the additional information field is not including the Called-Station-Id AVP and correct it to include the APN. Or have that policy client include another binding correlation key that can be used to find the binding.
3. Examine associated measurements RxBindCapMissingApn and RxBindDepMissingApn.
4. If the problem persists, contact My Oracle Support (MOS).
Charging Proxy Application (CPA) Alarms and Events (22800-22849)

22804 - Number of cSBR Unavailable Subresources at Threshold

Alarm Type: CPA
Description: The number of unavailable SBR subresources meets or exceeds the CpaSbrForUnavailable engineering configurable threshold.
Severity: Critical
Instance: Site Id
HA Score: Normal
Auto Clear Seconds: N/A
OID: eagleXgDiameterCpaUnavailableSubresourcesAtThreshold
Recovery:
1. Check the state of the SBR MPs.
   One or more Charging SBR subresources are unavailable. Make sure the SBR MPs are not having networking trouble.
2. Contact *My Oracle Support (MOS)* for assistance.

22805 - Message Decoding Failure

Event Type: CPA
Description: The CPA application could not decode a received Diameter message
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgDiameterCpaMsgDecodeFailureNotify
Recovery:
1. 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.
   While parsing the message, the message content was inconsistent with the "Message Length" in the message header.
2. Contact *My Oracle Support (MOS)* for assistance.
22806 - Unknown Diameter Application Id

Event Type: CPA

Description: The CPA application received a Diameter message with an unexpected DSR application id. The DSR Relay Agent forwarded a Request message to the CPA application which contained an unrecognized Diameter Application ID in the header. A DSR Relay Agent application routing rule is mis-provisioned.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnknownAppIdNotify

Recovery:
1. Examine the DSR Relay Agent application routing rule for provisioning errors.
   The currently provisioned Application Routing Rules can be viewed using Main Menu > Diameter > Configuration > Application Routing Rules.
2. Contact My Oracle Support (MOS) for assistance.

22807 - Unknown Command Code

Event Type: CPA

Description: The CPA application received a Diameter message other than an Accounting message. The Command Code received in the Diameter message is not an Accounting Message. A DSR Relay Agent application routing rule is mis-provisioned.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnknownCmdCodeNotify

Recovery:
1. Examine the DSR Relay Agent application routing rule for provisioning errors.
   The currently provisioned Application Routing Rules can be viewed using Main Menu > Diameter > Configuration > Application Routing Rules.
2. Contact My Oracle Support (MOS) for assistance.

22808 - Session Not Found

Event Type: CPA
Description: The CPA queried the SBR and did not get a match for a Session Binding Record based on the session id. The CPA application expected a Session Binding Record but did not find one. This condition might indicate that the SBR has timed out the record and deleted it.

Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 20
OID: eagleXgDiameterCpaSessionNotFoundNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance.

22809 - Undelivered SBR Query

Event Type: CPA

Description: The ComAgent could not deliver the SBR query or no response was received from the SBR. This event is generated when the ComAgent times out an SBR query because it could not deliver it or no response was received from the far end.

Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgDiameterCpaUndeliveredSbrQueryNotify
Recovery:
1. Make sure the SBR MPs are not having networking trouble.
2. Contact My Oracle Support (MOS) for assistance.

22810 - Routing attempt failed due to internal resource exhaustion

Event Type: CPA

Description: An attempt to route a Diameter message through the DRL has failed due to resource exhaustion.

Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgDiameterCpaRteFailResourceExhNotify
Recovery:
1. The MP may be experiencing local congestion.
2. Contact *My Oracle Support (MOS)* for assistance.

### 22811 - CPA Application Event Task Queue Utilization

**Event Type:** CPA  
**Description:** The CPA Application’s Event Queue Utilization is approaching its maximum capacity. The DSR Application’s Event Queue (which processes SBR responses that are sent via ComAgent) is approaching its maximum capacity.  
**Severity:** Minor, Major, Critical  
**Instance:** CPA  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterCpaAppEventQueueUtilNotify  
**Recovery:**  
1. The alarm log should be examined using Main Menu > Alarms & Events.  
   If no additional congestion alarms are indicated, the CPA Event Task may be experiencing a problem preventing it from processing messages from its Event Queue.  
2. If this problem persists, contact *My Oracle Support (MOS)* for assistance.

### 22812 - Missing AVP

**Event Type:** CPA  
**Description:** A received Diameter Accounting message does not contain the required Accounting Record Type or Accounting Record Number AVP.  
**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Throttle Seconds:** 5  
**OID:** eagleXgDiameterCpaMissingAvpNotify  
**Recovery:**  
If this problem persists, contact *My Oracle Support (MOS)* for assistance.

### 22813 - Received an error response to an SBR Query

**Event Type:** CPA  
**Description:** CPA application received an error response in reply to an SBR query. An application specific error message was received in response to an SBR query.  
**Severity:** Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 20
OID: eagleXgDiameterCpaSbrErrorRespNotify
Recovery:
    If this problem persists, contact My Oracle Support (MOS) for assistance.

22814 - HA Sub-Resource Unavailable

Event Type: CPA
Description: An HA Sub-Resource corresponding to a partition of the Session Binding Repository is unavailable. CPA has received a callback from ComAgent indicating that an HA sub-resource is unavailable.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgDiameterCpaHASubResourceUnavailableNotify
Recovery:
    If this problem persists, contact My Oracle Support (MOS) for assistance.

22815 - Unexpected Session

Event Type: CPA
Description: A Session Binding Record was found when none was expected. CPA received an ACA-Start and found a Session Binding Record already exists.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgDiameterCpaUnexpectedSessionNotify
Recovery:
    If this problem persists, contact My Oracle Support (MOS) for assistance.

22816 - One or more cSBR Subresources Unavailable

Alarm Type: CPA
Description: One or more Charging SBR Subresources are unavailable.

Severity: Based on Subresources unavailable.
- Major - one or more (but not all) cSBR Subresources are unavailable.
- Critical - all cSBR Subresources are unavailable.

Instance: Site Id

HA Score: Normal

Auto Clear Seconds: N/A

OID: eagleXgDiameterCpaSbrSubresourceIsUnavailableNotify

Recovery:
1. Check the state of the SBR MPs.
   One or more Charging SBR subresources are unavailable. Make sure the SBR MPs are not having networking trouble.
2. Contact My Oracle Support (MOS) for assistance.

Tekelec Virtual Operating Environment, TVOE (24400-24499)

This section provides information and recovery procedures for the Tekelec Virtual Operation Environment (TVOE) alarms, ranging from 24400-24499.

24400 - TVOE libvirtd is down

Alarm Type: TVOE

Description: This alarm indicates that the libvirtd daemon is not running.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.1

Recovery:
If the problem persists, contact My Oracle Support (MOS).

24401 - TVOE libvirtd is hung

Alarm Type: TVOE

Description: This alarm indicates that we attempted to determine if the libvirtd daemon is not responding and it didn’t respond.

Severity: Major
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.2
Recovery:
If the problem persists, contact My Oracle Support (MOS).

24402 - all TVOE libvirtd connections are in use

Alarm Type: TVOE
Description: This alarm indicates that all twenty connections to libvirtd are in use and more could be killed.
Severity: Major
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.3
Recovery:
If the problem persists, 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 - Rule Template failed to be updated

Event Type: CAPM
Description: The Rule Template failed to update because of syntax errors. The Additional Info of the Historical alarm includes the name of the Rule Template that failed to be updated.

When the alarm is caused by CAPM Rule Template which contains a syntax error, it may not be raised immediately after applying the template, but may occur when the first Rule has been provisioned and committed.
Severity: Minor
Instance: <ruleset> or <ruleset:rule-id>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterCapmUpdateFailedNotify
Recovery:
1. Check the CAPM Rule Template and verify that the left-hand side term of each condition contains a valid Linking-AVP or Select expression.
   A typical problem can be a non-existing expression, or syntax error of a custom-defined Select expression. If the CAPM Rule Template contains a syntax error, create a new Rule Template by copying and modifying the existing one, then deleting the old Rule Template.
2. Verify also that the recently provisioned data of the Rule Template does not contain a syntax error, i.e., the regular expressions are correct, the fields expecting numbers contain only numbers, etc.

25001 - Action failed within the Rule Template

Event Type: CAPM
Description: When a new Rule Template is created, a failure occurs when performing the action.
Severity: Info
Instance: <ruleset> or <ruleset:rule-id>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterCapmActionFailedNotify
Recovery:
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 - Stop Rule Template processing after action failure

Event Type: CAPM
Description: When Action Error Handling is set to ‘immediately exit from the rule template’ for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped.
Severity: Info
Instance: <ruleset> or <ruleset:rule-id>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterCapmExitRuleFailedNotify
Recovery:
No action required.
25003 - Exit Trigger point after action failure

Event Type: CAPM

Description: When Action Error Handling is set to ‘immediately exit from the trigger point’ for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped (subsequent templates within the trigger point are also skipped).

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmExitTriggerFailedNotify

Recovery:
No action required.

OAM Alarm Management (25500-25899)

This section provides information and recovery procedures related for alarms and events related to OAM Alarm Management, ranging from 25500 - 25899, that can occur on the system. All events have a severity of Info.

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

25500 - No DA-MP Leader Detected Alarm

Alarm Type: DIAM

Description: This alarm occurs when no active DA-MP leaders have been detected.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterNoDaMpLeaderDetectedNotify

Recovery:
If the problem persists, contact My Oracle Support (MOS) for assistance.
25510 - Multiple DA-MP Leader Detected Alarm

Alarm Type: DIAM
Description: This alarm occurs when multiple active DA-MP leaders have been detected.
Severity: Critical
Instance: <NetworkElement>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMultipleDaMpLeadersDetectedNotify
Recovery:
If the problem persists, contact My Oracle Support (MOS) for assistance.

Platform (31000-32700)

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32700.

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 Event types see Alarm and event types.
- Description: describes the reason for the alarm
- Default Severity: the severity of the alarm. This severity may vary, depending on user-defined and specific application settings.
- OID: alarm identifier that appears in SNMP traps
- Alarm ID: alarm identifier that is used internally
- Recovery: provides any necessary steps for correcting or preventing the alarm

31000 - S/W fault

Alarm Type: SW
Description: Program impaired by s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrSwFaultNotify
Recovery:
1. Export event history for the given server and the given process.
2. Contact My Oracle Support (MOS).

31001 - S/W status

Alarm Type: SW
Description: Program status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrSwStatusNotify
Recovery:
No action required.

31002 - Process watchdog failure

Alarm Type: SW
Description: Process watchdog timed out
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrProcWatchdogFailureNotify
Recovery:
1. Export event history for the given server and the given process.
2. Contact My Oracle Support (MOS).

31003 - Tab thread watchdog failure

Alarm Type: SW
Description: Tab thread watchdog timed out
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrThreadWatchdogFailureNotify
Recovery:
1. Export event history for the given server and the given process.
2. Contact My Oracle Support (MOS).

31100 - Database replication fault

Alarm Type: SW
Description: The Database replication process is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbReplicationFaultNotify
Recovery:
1. Export event history for the given server and inetsync task.
2. Contact My Oracle Support (MOS).

31101 - Database replication to slave failure

Alarm Type: REPL
Description: Database replication to a slave Database has failed
Severity: Critical
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepToSlaveFailureNotify
Recovery:
1. Check IMI 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 Type: REPL
Description: Database replication from a master Database has failed
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepFromMasterFailureNotify
Recovery:
1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact My Oracle Support (MOS).
31103- DB Replication update fault

Alarm Type: REPL
Description: Database replication process cannot apply update to DB
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepUpdateFaultNotify
Recovery:
1. Export event history for the given server and inetsync task.
2. Contact My Oracle Support (MOS).

31104 - DB Replication latency over threshold

Alarm Type: REPL
Description: Database replication latency has exceeded thresholds
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepLatencyNotify
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, contact My Oracle Support (MOS).

31105 - Database merge fault

Alarm Type: SW
Description: The database merge process (inetmerge) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbMergeFaultNotify
Recovery:
1. Export event history for the given server and inetmerge task.
2. Contact My Oracle Support (MOS).
31106 - Database merge to parent failure

Alarm Type: COLL
Description: Database merging to the parent Merge Node has failed
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrDbMergeToParentFailureNotify
Recovery:
1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact My Oracle Support (MOS).

31107 - Database merge from child failure

Alarm Type: COLL
Description: Database merging from a child Source Node has failed
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbMergeFromChildFailureNotify
Recovery:
1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact My Oracle Support (MOS).

31108 - Database merge latency over threshold

Alarm Type: COLL
Description: Database Merge latency has exceeded thresholds
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbMergeLatencyNotify
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, contact My Oracle Support (MOS)
31109 - Topology config error

Alarm Type: DB
Description: Topology is configured incorrectly
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrTopErrorNotify
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, contact My Oracle Support (MOS).

31110 - Database audit fault

Alarm Type: SW
Description: The Database service process (idbsvc) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbAuditFaultNotify
Recovery:
1. Export event history for the given server and idbsvc task.
2. Contact My Oracle Support (MOS).

31111 - Database merge audit in progress

Alarm Type: COLL
Description: Database Merge Audit between mate nodes in progress
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbMergeAuditNotify
Recovery:
   No action required.
31112 - Stateful db synchronization from mate server

Alarm Type: REPL
Description: Stateful database is not yet synchronized with mate database.
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 30
OID: eagleXgDsrDbRepUpLogTransTimeoutNotify
Recovery:
   No action required. Contact My Oracle Support (MOS) if this occurs frequently.

31113 - DB replication manually disabled

Alarm Type: REPL
Description: DB Replication Manually Disabled
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrDbReplicationManuallyDisabledNotify
Recovery:
   No action required.

31114 - DB replication over SOAP has failed

Alarm Type: REPL
Description: Database replication of configuration data via SOAP has failed
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 3600
OID: eagleXgDsrDbReplicationSoapFaultNotify
Recovery:
   1. Check IMI network connectivity between the affected servers.
   2. If there are no issues with network connectivity, contact My Oracle Support (MOS).

31115 - Database service fault

Alarm Type: SW
Description: The Database service process (idbsvc) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbServiceFaultNotify
Recovery:
1. Export event history for the given server and idbsvc task.
2. Contact My Oracle Support (MOS).

31116 - Excessive shared memory
Alarm Type: MEM
Description: The amount of shared memory consumed exceeds configured thresholds
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrExcessiveSharedMemoryConsumptionNotify
Recovery:
  Contact My Oracle Support (MOS).

31117 - Low disk free
Alarm Type: DISK
Description: The amount of free disk is below configured thresholds
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrLowDiskFreeNotify
Recovery:
1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact My Oracle Support (MOS).

31118 - Database disk store fault
Alarm Type: DISK
Description: Writing the database to disk failed
Severity: Minor
31119 - Database updatelog overrun

Alarm Type: DB
Description: The Database update log was overrun increasing risk of data loss
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbUpdateLogOverrunNotify
Recovery:
   Contact *My Oracle Support (MOS)*.

31120 - Database updatelog write fault

Alarm Type: DB
Description: A Database change cannot be stored in the updatelog
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbUpdateLogWriteFaultNotify
Recovery:
   Contact *My Oracle Support (MOS)*.

31121 - Low disk free early warning

Alarm Type: DISK
Description: The amount of free disk is below configured early warning thresholds
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrLowDiskFreeEarlyWarningNotify
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, contact My Oracle Support (MOS).

31122 - Excessive shared memory early warning

Alarm Type: MEM
Description: The amount of shared memory consumed exceeds configured early warning thresholds
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrExcessiveShMemConsumptionEarlyWarnNotify
Recovery:
  Contact My Oracle Support (MOS).

31123 - Database replication audit command complete

Alarm Type: REPL
Description: ADIC found one or more errors that are not automatically fixable.
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepAuditCmdCompleteNotify
Recovery:
  No action required.

31124 - ADIC error

Alarm Type: REPL
Description: An ADIC detected errors
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepAuditCmdErrNotify
Recovery:
  Contact My Oracle Support (MOS).
31125 - Database durability degraded

Alarm Type: REPL
Description: Database durability has dropped below configured durability level
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbDurabilityDegradedNotify
Recovery:
1. Check configuration of all servers, and check for connectivity problems between server IMI addresses.
2. If the problem persists, contact My Oracle Support (MOS).

31126 - Audit blocked

Alarm Type: REPL
Description: Site Audit Controls blocked an inter-site replication audit due to the number in progress per configuration.
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrAuditBlockedNotify
Recovery:
Contact My Oracle Support (MOS).

31127 - DB Replication Audit Complete

Alarm Type: REPL
Description: DB replication audit completed
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbRepAuditCompleteNotify
Recovery:
No action required.
31128 - ADIC Found Error

Alarm Type: REPL
Description: ADIC found one or more errors that are not automatically fixable.
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbADICErrorNotify
Recovery:
   Contact My Oracle Support (MOS).

31129 - ADIC Found Minor Issue

Alarm Type: REPL
Description: ADIC found one or more minor issues that can most likely be ignored
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 14400
OID: eagleXgDsrDbADICWarn
Recovery:
   No action required.

31130 - Network health warning

Alarm Type: NET
Description: Network health issue detected
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrNetworkHealthWarningNotify
Recovery:
1. Check configuration of all servers, and check for connectivity problems between server IMI addresses.
2. If the problem persists, contact My Oracle Support (MOS).
31131 - IDB Throttled for Extended Period

Alarm Type: DB
Description: IDB has one or more processes throttled for an extended period.
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: OustedThrottleWarnNotify
Recovery:
1. Monitor for workload in excess of documented capacity.
2. Contact My Oracle Support (MOS) if this alarm persists.

31140 - Database perl fault

Alarm Type: SW
Description: Perl interface to Database is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbPerlFaultNotify
Recovery:
Contact My Oracle Support (MOS).

31145 - Database SQL fault

Alarm Type: SW
Description: SQL interface to Database is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbSQLFaultNotify
Recovery:
1. Export event history for the given server, and lmysqld task.
2. Contact My Oracle Support (MOS).
31146 - DB mastership fault

Alarm Type: SW
Description: DB replication is impaired due to no mastering process (inetrep/inetrep).
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbMastershipFaultNotify
Recovery:
1. Export event history for the given server.
2. Contact My Oracle Support (MOS).

31147 - DB upsynclog overrun

Alarm Type: SW
Description: UpSyncLog is not big enough for (WAN) replication.
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbUpSyncLogOverrunNotify
Recovery:
   Contact My Oracle Support (MOS).

31148 - DB lock error detected

Alarm Type: DB
Description: The DB service process (idbsvc) has detected an IDB lock-related error caused by another process. The alarm likely indicates a DB lock-related programming error, or it could be a side effect of a process crash.
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbLockErrorNotify
Recovery:
   Contact My Oracle Support (MOS).
31200 - Process management fault

**Alarm Type:** SW

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

**Severity:** Minor

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** eagleXgDsrProcMgmtFaultNotify

**Recovery:**
1. Export event history for the given server, all processes.
2. Contact *My Oracle Support (MOS).*

31201 - Process not running

**Alarm Type:** PROC

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

**Severity:** Major

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** eagleXgDsrProcNotRunningNotify

**Recovery:**
1. Contact *My Oracle Support (MOS).*

31202 - Unkillable zombie process

**Alarm Type:** PROC

**Description:** A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.

**Severity:** Major

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** eagleXgDsrProcZombieProcessNotify

**Recovery:**
1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. Contact *My Oracle Support (MOS).*
31206 - Process mgmt monitoring fault

Alarm Type: SW
Description: The process manager monitor (pm.watchdog) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrProcMgmtMonFaultNotify
Recovery:
   Contact My Oracle Support (MOS).

31207 - Process resource monitoring fault

Alarm Type: SW
Description: The process resource monitor (ProcWatch) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrProcResourceMonFaultNotify
Recovery:
   Contact My Oracle Support (MOS).

31208 - IP port server fault

Alarm Type: SW
Description: The run environment port mapper (re.portmap) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrPortServerFaultNotify
Recovery:
   Contact My Oracle Support (MOS).

31209 - Hostname lookup failed

Alarm Type: SW
Description: Unable to resolve a hostname specified in the NodeInfo table
Severity: Minor  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrHostLookupFailedNotify  
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, contact My Oracle Support (MOS).

31213 - Process scheduler fault

Alarm Type: SW
Description: The process scheduler (ProcSched/runat) is impaired by a s/w fault
Severity: Minor  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrProcSchedulerFaultNotify  
Recovery:  
  Contact My Oracle Support (MOS).

31214 - Scheduled process fault

Alarm Type: PROC
Description: A scheduled process cannot be executed or abnormally terminated
Severity: Minor  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrScheduleProcessFaultNotify  
Recovery:  
  Contact My Oracle Support (MOS).

31215 - Process resources exceeded

Alarm Type: SW
Description: A process is consuming excessive system resources
Severity: Minor  
HA Score: Normal
Auto Clear Seconds: 14400
OID: eagleXgDsrProcResourcesExceededFaultNotify
Recovery:
   Contact My Oracle Support (MOS).

31216 - SysMetric configuration error
   Alarm Type: SW
   Description: A SysMetric Configuration table contains invalid data
   Severity: Minor
   HA Score: Normal
   Auto Clear Seconds: 300
   OID: eagleXgDsrSysMetricConfigErrorNotify
   Recovery:
      Contact My Oracle Support (MOS).

31220 - HA configuration monitor fault
   Alarm Type: SW
   Description: The HA configuration monitor is impaired by a s/w fault
   Severity: Minor
   HA Score: Normal
   Auto Clear Seconds: 300
   OID: eagleXgDsrHaCfgMonitorFaultNotify
   Recovery:
      Contact My Oracle Support (MOS).

31221 - HA alarm monitor fault
   Alarm Type: SW
   Description: The high availability alarm monitor is impaired by a s/w fault
   Severity: Minor
   HA Score: Normal
   Auto Clear Seconds: 300
   OID: eagleXgDsrHaAlarmMonitorFaultNotify
   Recovery:
31222 - HA not configured

Alarm Type: HA  
Description: High availability is disabled due to system configuration  
Severity: Minor  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrHaNotConfiguredNotify  
Recovery:  
Contact My Oracle Support (MOS).

31223 - HA Heartbeat transmit failure

Alarm Type: HA  
Description: The high availability monitor failed to send heartbeat  
Severity: Major  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrHaHbTransmitFailureNotify  
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, contact My Oracle Support (MOS).

31224 - HA configuration error

Alarm Type: HA  
Description: High availability configuration error  
Severity: Major  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrHaCfgErrorNotify  
Recovery:  
Contact My Oracle Support (MOS).
31225 - HA service start failure

Alarm Type: HA
Description: The high availability service failed to start
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaSvcStartFailureNotify
Recovery:
1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, contact My Oracle Support (MOS).

31226 - HA availability status degraded

Alarm Type: HA
Description: The high availability status is degraded due to raised alarms
Severity: Major
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaAvailDegradedNotify
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).

31227 - HA availability status failed

Alarm Type: HA
Description: The high availability status is failed due to raised alarms
Severity: Critical
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaAvailFailedNotify
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

Alarm Type: HA
Description: High availability standby server is offline
Severity: Major
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrHaStandbyOfflineNotify
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 Contact My Oracle Support (MOS).

31229 - HA score changed

Alarm Type: HA
Description: High availability health score changed
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaScoreChangeNotify
Recovery:
Status message - no action required.

31230 - Recent alarm processing fault

Alarm Type: SW
Description: The recent alarm event manager (raclerk) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrRecAlarmEvProcFaultNotify
Recovery:
1. Export event history for the given server and raclerk task.
2. Contact My Oracle Support (MOS).
31231 - Platform alarm agent fault

Alarm Type: SW  
Description: The platform alarm agent impaired by a s/w fault  
Severity: Minor  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrPlatAlarmAgentNotify  
Recovery:  
Contact My Oracle Support (MOS).

31232 - Late heartbeat warning

Alarm Type: HA  
Description: High availability server has not received a heartbeat within the configured interval.  
Severity: Minor  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrHaLateHeartbeatWarningNotify  
Recovery:  
No action required; this is a warning and can be due to transient conditions. If there continues to be no heartbeat from the server, alarm 31228 occurs.

31233 - HA Secondary Path Down

Alarm Type: HA  
Description: High availability secondary path loss of connectivity  
Severity: Major  
HA Score: Normal  
Auto Clear Seconds: 300  
OID: eagleXgDsrHaPathDownNotify  
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. Contact My Oracle Support (MOS).
31234 - Untrusted Time Upon Initialization

Alarm Type: REPL

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

Severity: Critical

Instance:

Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrUtrustedTimeOnInitNotify

Recovery:
1. Correct NTP configuration.
2. If the problem persists, contact My Oracle Support (MOS).

31235 - Untrusted Time After Initialization

Alarm Type: REPL

Description: After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, etc. There are often accompanying Platform alarms to guide correction. Generally, applications remaining be running, but time-stamped data is likely incorrect, reports may be negatively affected, some behavior may be improper, etc.

Severity: Critical

Instance:

Auto Clear Seconds: 0
OID: eagleXgDsrUtrustedTimePostInitNotify

Recovery:
1. Correct NTP configuration.
2. If the problem persists, contact My Oracle Support (MOS).

31236 - HA Link Down

Alarm Type: HA

Description: High availability TCP link is down.

Severity: Critical

Instance: Remote node being connected to plus the path identifier
HA Score: Normal
Auto Clear Seconds: 300
OID: HaLinkDownNotify

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

31240 - Measurements collection fault

Alarm Type: SW
Description: The measurements collector (statclerk) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrMeasCollectorFaultNotify

Recovery:
1. Export event history for the given server and statclerk task.
2. Contact My Oracle Support (MOS).

31250 - RE port mapping fault

Alarm Type: SW
Description: The IP service port mapper (re.portmap) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrRePortMappingFaultNotify

Recovery:
This typically indicate a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.

31260 - Database SNMP Agent

Alarm Type: SW
Description: The Database SNMP agent (snmpIdbAgent) is impaired by a s/w fault
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrDbSnmpAgentNotify

Recovery:
1. Export event history for the given server and all processes.
2. Contact My Oracle Support (MOS).

31270 - Logging output

Alarm Type: SW
Description: Logging output set to Above Normal
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrLoggingOutputNotify

Recovery:
Extra diagnostic logs are being collected, potentially degrading system performance. Contact My Oracle Support (MOS).

31280 - HA Active to Standby transition

Alarm Type: HA
Description: HA active to standby activity transition
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrActiveToStandbyTransNotify

Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31281 - HA Standby to Active transition

Alarm Type: HA
Description: HA standby to active activity transition
Severity: Info
31282 - HA Management Fault

Alarm Type: HA
Description: The HA manager (cmha) is impaired by a software fault.
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaMgmtFaultNotify
Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31283 - HA Server Offline

Alarm Type: HA
Description: High availability server is offline
Severity: Critical
HA Score: Normal
Auto Clear Seconds: 0
OID: eagleXgDsrHaServerOfflineNotify
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 Contact My Oracle Support (MOS).

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Type: HA
Description: High availability remote subscriber has not received a heartbeat within the configured interval.
Severity: Minor
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaRemoteHeartbeatWarningNotify
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, contact My Oracle Support (MOS).

31285 - HA Split Brain Recovery Entry
Alarm Type: HA
Description: High availability split brain recovery entered
Severity: Info
Instance: Cluster set key of the DC outputting the event
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaSbrEntryNotify
Recovery:
No action required; this is a status message generated when one or more unaccounted for nodes join the designated coordinators group.

31286 - HA Split Brain Recovery Plan
Alarm Type: HA
Description: High availability split brain recovery plan
Severity: Info
Instance: Names of HA Policies (as defined in HA policy configuration)
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaSbrPlanNotify
Recovery:
No action required; this is a status message output when the designated coordinator generates a new action plan during split brain recovery.

31287 - HA Split Brain Recovery Complete
Alarm Type: HA
Description: High availability split brain recovery complete
Severity: Info
Instance: Names of HA Policies (as defined in HA policy configuration)
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaSbrCompleteNotify
Recovery:
No action required; this is a status message output when the designated coordinator finishes running an action plan during split brain recovery.

31290 - HA Process Status
Alarm Type: HA
Description: HA manager (cmha) status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaProcessStatusNotify
Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31291 - HA Election Status
Alarm Type: HA
Description: HA DC Election status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaElectionStatusNotify
Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31292 - HA Policy Status
Alarm Type: HA
**Description:** HA Policy plan status  
**Severity:** Info  
**HA Score:** Normal  
**Auto Clear Seconds:** 300  
**OID:** eagleXgDsrHaPolicyStatusNotify  
**Recovery:**  
1. If this alarm occurs during routine maintenance activity, it may be ignored.  
2. Otherwise, contact *My Oracle Support (MOS).*

**31293 - HA Resource Link Status**  
**Alarm Type:** HA  
**Description:** HA ResourceAgent Link status  
**Severity:** Info  
**HA Score:** Normal  
**Auto Clear Seconds:** 300  
**OID:** eagleXgDsrHaRaLinkStatusNotify  
**Recovery:**  
1. If this alarm occurs during routine maintenance activity, it may be ignored.  
2. Otherwise, contact *My Oracle Support (MOS).*

**31294 - HA Resource Status**  
**Alarm Type:** HA  
**Description:** HA Resource registration status  
**Severity:** Info  
**HA Score:** Normal  
**Auto Clear Seconds:** 300  
**OID:** eagleXgDsrHaResourceStatusNotify  
**Recovery:**  
1. If this alarm occurs during routine maintenance activity, it may be ignored.  
2. Otherwise, contact *My Oracle Support (MOS).*

**31295 - HA Action Status**  
**Alarm Type:** HA  
**Description:** HA Resource action status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaActionStatusNotify

Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31296 - HA Monitor Status
Alarm Type: HA
Description: HA Monitor action status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaMonitorStatusNotify

Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31297 - HA Resource Agent Info
Alarm Type: HA
Description: HA Resource Agent Info
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaRaInfoNotify

Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact My Oracle Support (MOS).

31298 - HA Resource Agent Detail
Alarm Type: HA
Description: Resource Agent application detailed information
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaRaDetailNotify
Recovery:
1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact *My Oracle Support (MOS).*

**31299 - HA Notification Status**

Alarm Type: HA
Description: HA Notification status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaNotificationNotify
Recovery:
No action required.

**31300 - HA Control Status**

Alarm Type: HA
Description: HA Control action status
Severity: Info
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDsrHaControlNotify
Recovery:
No action required.

**32100 - Breaker Panel Feed Unavailable**

Alarm Type: PLAT
Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Default Severity: Critical
OID: eagleXgDsrTpdBrkPnlFeedUnavailableNotify

E53474 Revision 01, July 2014
Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdBrkPnlBreakerFailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32102 - Breaker Panel Maint Failure

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdBrkPnlMntFailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32103 - Power Feed Unavailable

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdPowerFeedUnavailNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Type: PLAT
Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdPowerSupply1FailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdPowerSupply2FailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdPowerSupply3FailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32107 - Raid Feed Unavailable

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdRaidFeedUnavailableNotify

Recovery
Contact My Oracle Support (MOS) to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Type: PLAT
Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Default Severity: Critical
OID: eagleXgDsrTpdRaidPower1FailureNotify
Recovery
Contact My Oracle Support (MOS) to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Type: PLAT
Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Default Severity: Critical
OID: eagleXgDsrTpdRaidPower2FailureNotify
Recovery
Contact My Oracle Support (MOS) to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Type: PLAT
Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Default Severity: Critical
OID: eagleXgDsrTpdRaidPower3FailureNotify
Recovery
Contact My Oracle Support (MOS) to request hardware replacement.

32111 - Device Failure

Alarm Type: PLAT
Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdeviceFailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32112 - Device Interface Failure

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdeviceIfFailureNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32113 - Uncorrectable ECC memory error

Alarm Type: TPD

Description: This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdeviceEccUncorrectableErrorNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32114 - SNMP get failure

Alarm Type: TPD

Description: The server failed to receive SNMP information from the switch.

Severity: Critical
32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Type: TPD

This alarm indicates that the server’s current time precedes the timestamp of the last known time the server's time was good.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdNTPDaemonNotSynchronizedFailureNotify

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. If the problem persists, contact My Oracle Support (MOS).

32116 - TPD Server's Time Has Gone Backwards

Alarm Type: TPD

This alarm indicates that the server’s current time precedes the timestamp of the last known time the server's time was good.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdNTPTimeGoneBackwardsNotify

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**32117 - TPD NTP Offset Check Failure**

**Alarm Type:** TPD

This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold

**Severity:** Critical

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

**HA Score:** Normal

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

**OID:** eagleXgDsrNtpOffsetCheckFailureNotify

**Recovery:**

1. Run syscheck in verbose mode.
2. Contact *My Oracle Support (MOS)*.

**32300 – Server fan failure**

**Alarm Type:** TPD

**Description:** This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

**Severity:** Major

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdFanErrorNotify

**Recovery**

Contact *My Oracle Support (MOS)*.

**32301 - Server internal disk error**

**Alarm Type:** TPD

**Description:** This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server’s disks has either failed or is approaching failure.

**Severity:** Major


### 32302 – Server RAID disk error

**Alarm Type:** TPD  
**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:** eagleXgDsrTpdIntDiskErrorNotify  
**Recovery**  
Contact *My Oracle Support (MOS)*.

### 32303 - Server Platform error

**Alarm Type:** TPD  
**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:** eagleXgDsrTpdRaidDiskErrorNotify  
**Recovery**  
Contact *My Oracle Support (MOS)* and provide the system health check output.

### 32304 - Server file system error

**Alarm Type:** TPD
**Description:** This alarm indicates unsuccessful writing to at least one of the server’s file systems.

**Severity:** Major

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdFileSystemErrorNotify

**Recovery**

Contact *My Oracle Support (MOS).*

---

**32305 - Server Platform process error**

**Alarm Type:** TPD

**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:** eagleXgDsrTpdPlatProcessErrorNotify

**Recovery**

Contact *My Oracle Support (MOS).*

---

**32306 – Server RAM shortage error**

**Alarm Type:** TPD

Not Implemented.

**Severity:** Major

**OID:** eagleXgDsrTpdRamShortageErrorNotify

Contact *My Oracle Support (MOS).*

---

**32307 - Server swap space shortage failure**

**Alarm Type:** TPD

**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
### 32308 - Server provisioning network error

**Alarm Type:** TPD

**Description:** This alarm indicates that the connection between the server’s ethernet interface and the customer network is not functioning properly.

**Severity:** Major

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdProvNetworkErrorNotify

**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, contact *My Oracle Support (MOS)*.

### 32309 - Eagle Network A Error

**Alarm Type:** PLAT

**Description:** Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

**Default Severity:** Critical

**OID:** eagleXgDsrTpdEagleNetworkAErrorNotify

**Recovery**

Contact *My Oracle Support (MOS)* to request hardware replacement.
32310 - Eagle Network B Error

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdEagleNetworkBErrorNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32311 - Sync Network Error

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: eagleXgDsrTpdSyncNetworkErrorNotify

Recovery

Contact My Oracle Support (MOS) to request hardware replacement.

32312 - Server disk space shortage error

Alarm Type: TPD

Description: This alarm indicates that one of the following conditions has occurred:

- A filesystem has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the filesystem.
- More than 90% of the total number of available files have been allocated on the filesystem.
- A filesystem has a different number of blocks than it had when installed.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDiskSpaceShortageErrorNotify

Recovery

Contact My Oracle Support (MOS).
32313 - Server default route network error

Alarm Type: TPD

Description: This alarm indicates that the default network route of the server is experiencing a problem.

Caution: When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDefaultRouteNetworkErrorNotify

Recovery

Contact My Oracle Support (MOS).

32314 - Server temperature error

Alarm Type: TPD

Description: The internal temperature within the server is unacceptably high.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdTemperatureErrorNotify

Recovery

1. Ensure that nothing is blocking the fan's 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. If the problem has not been resolved, contact My Oracle Support (MOS).
32315 – Server mainboard voltage error

Alarm Type: TPD

Description: This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpDMainboardVoltageErrorNotify

Recovery

Contact My Oracle Support (MOS).

32316 – Server power feed error

Alarm Type: TPD

Description: This alarm indicates that one of the power feeds to the server has failed. If this alarm occurs in conjunction with any Breaker Panel alarm, there might be a problem with the breaker panel.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpDPowerFeedErrorNotify

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, contact My Oracle Support (MOS).

32317 - Server disk health test error

Alarm Type: TPD
Description: Either the hard drive has failed or failure is imminent.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdDiskHealthErrorNotify

Recovery
1. Perform the recovery procedures for the other alarms that accompany this alarm.
2. If the problem has not been resolved, contact My Oracle Support (MOS).

32318 - Server disk unavailable error

Alarm Type: TPD
Description: The smartd service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdDiskUnavailableErrorNotify

Recovery
   Contact My Oracle Support (MOS).

32319 – Device error

Alarm Type: TPD
This alarm indicates that the offboard storage server had a problem with its disk volume filling up.
Severity: Major
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdDeviceErrorNotify
Recovery
  Contact My Oracle Support (MOS).

32320 – Device interface error

Alarm Type: TPD
Description: This alarm indicates that the IP bond is either not configured or down.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdDeviceIfErrorNotify
Recovery
  Contact My Oracle Support (MOS).

32321 – Correctable ECC memory error

Alarm Type: TPD
Description: This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdEccCorrectableErrorNotify
Recovery
  No recovery necessary. If the condition persists, contact My Oracle Support (MOS) to request hardware replacement.

32322 – Power Supply A error

Alarm Type: TPD
Description: This alarm indicates that power supply 1 (feed A) has failed.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdPowerSupply1ErrorNotify
Recovery
1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact My Oracle Support (MOS).

32323 – Power Supply B error

Alarm Type: TPD
Description: This alarm indicates that power supply 2 (feed B) has failed.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdPowerSupply2ErrorNotify
Recovery
1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact My Oracle Support (MOS).

32324 – Breaker panel feed error

Alarm Type: TPD
Description: This alarm indicates that the server is not receiving information from the breaker panel relays.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdBrkPnlFeedErrorNotify
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, contact My Oracle Support (MOS) to request that the breaker panel be replaced.

32325 - Breaker panel breaker error

Alarm Type: TPD

Description: This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see Figure 4: Breaker Panel LEDs) identify whether the fault occurred on the input power or the output power, as follows:

• A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit.

Note: LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.

• A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.

Figure 4: Breaker Panel LEDs

Description: This alarm indicates that a power fault has been identified by the breaker panel.
Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdBrkPnlBreakerErrorNotify

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. Look at the breaker panel assignments and verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

   ![Figure 5: Breaker Panel Setting](image)

   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. Contact the My Oracle Support (MOS)

   a) 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.

   b) Check the LEDs in the PWR BUS A group and the PWR BUS B group again.
      - If the LEDs are now illuminated Green, the issue has been resolved.
      - Proceed to Substep c to verify that the alarm has been cleared.
      - If the LEDs are still illuminated Red, continue to the next sub-step.

   c) 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.
d) 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.

- If the LEDs are now illuminated Green, the issue has been resolved. Proceed to Step 3 to verify that the alarm has been cleared.
- If the LEDs are still illuminated Red, skip to Step 4

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, Contact the My Oracle Support (MOS)

- 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, continue with the next step.
- 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 Contact the My Oracle Support (MOS)

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 problem has not been resolved, contact My Oracle Support (MOS)

32326 – Breaker panel monitoring error

Alarm Type: TPD

Description: This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself.

Note: When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm 32324-Breaker Panel Feed Error or 32325-Breaker Panel Breaker Error until the Breaker Panel Monitoring Error has been corrected.

Severity: Major

Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpDbkPnlMntErrorNotify

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 both ends of the labeled serial cables are secured properly (for locations of serial cables,
   see the appropriate hardware manual).
3. If the alarm has not been cleared, contact My Oracle Support (MOS).

32327 – Server HA Keepalive error

Alarm Type: TPD
Description: This alarm indicates that heartbeat process has detected that it has failed to receive a
heartbeat packet within the timeout period.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and
   bindVarNamesValueStr

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.

32328 – DRBD is unavailable

Alarm Type: TPD
Description: This alarm indicates that DRBD is not functioning properly on the local server. The DRBD
state (disk state, node state, and/or connection state) indicates a problem.
Severity: Major
OID: eagleXgDsrTpDrdbUnavailableNotify
Recovery

Contact My Oracle Support (MOS).

32329 – DRBD is not replicating

Alarm Type: TPD

Description: This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.

Severity: Major

OID: eagleXgDsrTpdDrbdNotReplicatingNotify

Recovery

Contact My Oracle Support (MOS).

32330 – DRBD peer problem

Alarm Type: PLAT

Description: This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.

Severity: Major

OID: eagleXgDsrTpdDrbdPeerProblemNotify

Recovery

Contact the My Oracle Support (MOS).

32331 – HP disk problem

Alarm Type: TPD

Description: This major alarm indicates that there is an issue with either a physical or logical disk in the HP disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdHpDiskProblemNotify

Recovery

Contact My Oracle Support (MOS).
32332 – HP Smart Array controller problem

**Alarm Type:** TPD

**Description:** This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.

**Severity:** Major

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdHpDiskCtrlrProblemNotify

**Recovery**

Contact *My Oracle Support (MOS)*.

32333 – HP hpacucliStatus utility problem

**Alarm Type:** TPD

**Description:** This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus daemon is either not running, or hung.

**Severity:** Major

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdHPACUCLIProblemNotify

**Recovery**

Contact *My Oracle Support (MOS)*.

32334 - Multipath device access link problem

**Alarm Type:** TPD

**Description:** One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

**Severity:** Major

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdMpathDeviceProblemNotify
32335 - Switch link down error

Alarm Type: TPD

Description: The link is down.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdSwitchLinkDownErrorNotify

Recovery

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, contact My Oracle Support (MOS) who should verify port settings on both the server and the switch.

32336 – Half Open Socket Limit

Alarm Type: TPD

Description: This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdHalfOpenSockLimitNotify

Recovery

Contact My Oracle Support (MOS).

32337 - E5-APP-B Firmware Flash

Alarm Type: TPD

Description: This alarm indicates there was an error while trying to update the firmware flash on the E5-APP-B cards.

Severity: Major

HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.38
Recovery:
   Contact My Oracle Support (MOS).

32338 - E5-APP-B Serial mezzanine seating
   Alarm Type: TPD
   Description: This alarm indicates the serial mezzanine board was not properly seated.
   Severity: Major
   HA Score: Normal
   Auto Clear Seconds: 0 (zero)
   OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.39
   Recovery:
   Contact My Oracle Support (MOS).

32339 - Max pid limit
   Alarm Type: TPD
   Description: This alarm indicates that the maximum number of running processes has reached the major threshold.
   Severity: Major
   Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
   HA Score: Normal
   Auto Clear Seconds: 0 (zero)
   OID: eagleXgDsrTpdMaxPidLimitNotify
   Recovery:
   1. Run syscheck in verbose mode.
   2. Contact My Oracle Support (MOS).

32340 - Server NTP Daemon Lost Synchronization
   Alarm Type: TPD
   Description: This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.
   Severity: Major
**32341 - Server NTP Daemon Never Synchronized Error**

**Alarm Type:** TPD  
**Description:** This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.  
**Severity:** Major  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDsrTpdNTPDaemonNeverSynchronizedNotify  
**Recovery:**  
1. Verify NTP settings and that NTP sources can be reached.  
2. Contact *My Oracle Support (MOS).*

**32342 - NTP Offset Check Error**

**Alarm Type:** TPD  
**Description:** This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.  
**Severity:** Major  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDsrNtpOffsetCheckErrorNotify  
**Recovery:**  
1. Verify NTP settings and that NTP are providing accurate time.  
2. Contact *My Oracle Support (MOS).*
32343 - RAID disk problem

Alarm Type: TPD
Description: This alarm indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdDiskProblemNotify
Recovery:
1. Run syscheck in verbose mode.
2. Contact My Oracle Support (MOS).

32344 - RAID controller problem

Alarm Type: TPD
Description: This alarm indicates that RAID controller needs intervention. State reported by syscheck is not "Normal" and/or BBU (backup battery unit) state is not "Operational".
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrTpdDiskCtrlrProblemNotify
Recovery:
1. Run syscheck in verbose mode.
2. Contact My Oracle Support (MOS).

32345 - Server Upgrade snapshot(s) invalid

Alarm Type: TPD
Description: This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
**Alarms and Events**

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdUpgradeSnapshotInvalidNotify

**Recovery:**
1. Run accept to remove invalid snapshot(s) and clear alarms.
2. Contact *My Oracle Support (MOS)*

### 32500 – Server disk space shortage warning

**Alarm Type:** TPD

**Description:** This alarm indicates that one of the following conditions has occurred:
- A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system.
- More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

**Severity:** Minor

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdDiskSpaceShortageWarningNotify

**Recovery**
- Contact *My Oracle Support (MOS)*.

### 32501 – Server application process error

**Alarm Type:** TPD

**Description:** This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

**Severity:** Minor

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdApplicationProcessErrorNotify

**Recovery**
- Contact *My Oracle Support (MOS)*.
32502 – Server hardware configuration error

**Alarm Type:** TPD

**Description:** This alarm indicates that one or more of the server’s hardware components are not in compliance with specifications (refer to the appropriate hardware manual).

**Severity:** Minor

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdHardwareConfigErrorNotify

**Recovery**

Contact *My Oracle Support (MOS).*

32503 – Server RAM shortage warning

**Alarm Type:** TPD

**Description:** This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

**Severity:** Minor

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdRamShortageWarningNotify

**Recovery**

Contact *My Oracle Support (MOS).*

32504 – Software Configuration Error

**Alarm Type:** PLAT

**Description:** This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

**Severity:** Minor

**OID:** eagleXgDsrTpdSoftwareConfigErrorNotify

**Recovery**

Contact *My Oracle Support (MOS).*
32505 – Server swap space shortage warning

Alarm Type: TPD

Description: This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

Note: For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdSwapSpaceShortageWarningNotify

Recovery

Contact My Oracle Support (MOS).

32506 – Server default router not defined

Alarm Type: TPD

Description: This alarm indicates that the default network route is either not configured or the current configuration contains an invalid IP address or hostname.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDefaultRouteNotDefinedNotify

Recovery

Contact My Oracle Support (MOS).

32507 – Server temperature warning

Alarm Type: TPD

Description: This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.

Severity: Minor
32508 – Server core file detected

Alarm Type: TPD

Description: This alarm indicates that an application process has failed and debug information is available.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdCoreFileDetectedNotify

Recovery

Contact My Oracle Support (MOS).

32509 – Server NTP Daemon not synchronized

Alarm Type: TPD

Description: This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity: Minor
**32510 – CMOS battery voltage low**

**Alarm Type:** TPD  
**Description:** The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.  
**Severity:** Minor  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDsrTpdCMOSBatteryVoltageLowNotify  
**Recovery**  
Contact *My Oracle Support (MOS).*

**32511 – Server disk self test warning**

**Alarm Type:** TPD  
**Description:** A non-fatal disk issue (such as a sector cannot be read) exists.  
**Severity:** Minor  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDsrTpdSmartTestWarnNotify  
**Recovery**  
Contact *My Oracle Support (MOS).*
32512 – Device warning

Alarm Type: TPD

Description: This alarm indicates that either we are unable to perform an snmpget command on the configured SNMP OID or the value returned failed the specified comparison operation.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDeviceWarnNotify

Recovery

Contact My Oracle Support (MOS).

32513 – Device interface warning

Alarm Type: TPD

Description: This alarm can be generated by either an SNMP trap or an IP bond error.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDeviceIfWarnNotify

Recovery

Contact My Oracle Support (MOS).

32514 – Server reboot watchdog initiated

Alarm Type: TPD

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: eagleXgDsrTpdWatchdogRebootNotify

Recovery

Contact My Oracle Support (MOS).

32515 – Server HA failover inhibited

Alarm Type: TPD

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: eagleXgDsrTpdHaInhibitedNotify

Recovery

Contact My Oracle Support (MOS).

32516 – Server HA Active to Standby transition

Alarm Type: TPD

Description: This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdHaActiveToStandbyTransNotify

Recovery

Contact My Oracle Support (MOS).

32517 – Server HA Standby to Active transition

Alarm Type: TPD

Description: This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

Severity: Minor
32518 – Platform Health Check failure

**Alarm Type:** TPD  
**Description:** This alarm is used to indicate a configuration error.  
**Severity:** Minor  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDsrTpdPlatformHealthCheckFailedNotify  
**Recovery**  
Contact *My Oracle Support (MOS).*

32519 – NTP Offset Check failure

**Alarm Type:** TPD  
**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:** eagleXgDsrNtpOffsetCheckFailedNotify  
**Recovery**  
Contact *My Oracle Support (MOS).*
32520 – NTP Stratum Check failure

Alarm Type: TPD

**Description:** This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

**Severity:** Minor

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

**HA Score:** Normal

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

**OID:** eagleXgDsrNtpStratumCheckFailedNotify

**Recovery**

Contact *My Oracle Support (MOS)*.

32521 – SAS Presence Sensor Missing

Alarm Type: TPD

**Description:** This alarm indicates that the T1200 server drive sensor is not working.

**Severity:** Minor

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

**HA Score:** Normal

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

**OID:** eagleXgDsrSasPresenceSensorMissingNotify

**Recovery**

Contact *My Oracle Support (MOS)* to get a replacement server.

32522 – SAS Drive Missing

Alarm Type: TPD

**Description:** This alarm indicates that the number of drives configured for this server is not being detected.

**Severity:** Minor

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

**HA Score:** Normal

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

Recovery

Contact My Oracle Support (MOS) to determine whether the issue is with a failed drive or failed configuration.

32523 – DRBD failover busy

Alarm Type: TPD

Description: This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it’s data is not up to date.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDrbdFailoverBusyNotify

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, contact My Oracle Support (MOS).

32524 – HP disk resync

Alarm Type: TPD

Description: This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdHpDiskResyncNotify

Recovery

Contact My Oracle Support (MOS).

32525 – Telco Fan Warning

Alarm Type: TPD

Description: This alarm indicates that the Telco switch has detected an issue with an internal fan.
Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdTelcoFanWarningNotify

Recovery

1. Contact My Oracle Support (MOS) to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.
2. 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

Alarm Type: TPD

Description: This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdTelcoTemperatureWarningNotify

Recovery

1. Lower the ambient air temperature around the switch as low as possible.
2. If problem persists, contact My Oracle Support (MOS).

32527 – Telco Power Supply Warning

Alarm Type: TPD

Description: This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdTelcoPowerSupplyWarningNotify
Recovery

1. Verify breaker wasn’t tripped.
2. If breaker is still good and problem persists, 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

Alarm Type: TPD

Description: This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: `eagleXgDsrTpdInvalidBiosValueNotify`

Recovery

Contact My Oracle Support (MOS).

32529– Server Kernel Dump File Detected

Alarm Type: TPD

Description: This alarm indicates that the kernel has crashed and debug information is available.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: `eagleXgDsrTpdServerKernelDumpFileDetectedNotify`

Recovery

Contact My Oracle Support (MOS).

32530– Server Upgrade Fail Detected

Alarm Type: TPD

Description: This alarm indicates that a TPD upgrade has failed.

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdServerUpgradeFailDetectedNotify

Recovery

Contact My Oracle Support (MOS).

32531– Half Open Socket Warning

Alarm Type: TPD

This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdHalfOpenSocketWarningNotify

Recovery

Contact My Oracle Support (MOS).

32532– Server Upgrade Pending Accept/Reject

Alarm Type: TPD

Description: This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdServerUpgradePendingAcceptNotify

Recovery

Follow the steps in the application's upgrade procedure for accepting or rejecting the upgrade.

32533 - Max pid warning

Alarm Type: TPD
Description: This alarm indicates that the maximum number of running processes has reached the minor threshold.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdMaxPidWarningNotify

Recovery:
1. Run syscheck in verbose mode.
2. Contact My Oracle Support (MOS).

32534 - NTP Source Server Is Not Able To Provide Correct Time

Alarm Type: TPD

Description: This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdNTPSourceIsBadNotify

Recovery:
1. Verify NTP settings and that NTP sources are providing accurate time.
2. Contact My Oracle Support (MOS).

32535 - RAID disk resync

Alarm Type: TPD

Description: This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity: Minor

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

HA Score: Normal
**Auto Clear Seconds:** 0 (zero)

**OID:** eagleXgDsrTpdDiskResyncNotify

**Recovery:**
1. Run syscheck in verbose mode
2. If this alarm persists for several hours (depending on a load of a server rebuild of array can take multiple hours to finish), contact *My Oracle Support (MOS)*.

### 32536 - Server Upgrade snapshot(s) warning

**Alarm Type:** TPD

**Description:** This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.

**Severity:** Minor

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

**HA Score:** Normal

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

**OID:** eagleXgDsrTpdUpgradeSnapshotWarningNotify

**Recovery:**
1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. Contact *My Oracle Support (MOS)*

### 32700 - Telco Switch Notification

**Alarm Type:** PLAT

**Description:** Telco Switch Notification

**Severity:** Info

**OID:** eagleXgDsrTpdTelcoSwitchNotificationNotify

**Recovery**
- 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

Alarm Group: DIWF
Description: DM-IWF application was unable to register for MAP-to-Diameter transaction service. No MAP-to-Diameter transactions can be routed to this DA-MP.
Severity: Critical
Instance: None
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDmiwfAppComagentProviderRegistrationFailureNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance.

33001 - Diameter-to-MAP Service Registration Failure on DA-MP

Alarm Group: DIWF
Description: DM-IWF application was unable to register for Diameter-to-MAP transaction service. Diameter-to-MAP transactions cannot be serviced by this DA-MP.
Severity: Critical
Instance: None
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDmiwfAppComagentUserRegistrationFailureNotify
Recovery:
   Contact My Oracle Support (MOS) for assistance.

33002 - DM-IWF DA-MP not associated with a Place

Alarm Group: DIWF
Description: DM-IWF DA-MP server is not associated with an AppWorks Place
Severity: Critical
Instance: None
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDmiwfAppServerPlaceFailureNotify
Recovery:
1. If the Server is not associated with an AppWorks place, Admin Disable DM-IWF on the DA-MP Server, add the Server to an appropriate AppWorks Place, and then Admin Enable DM-IWF on the DA-MP Server.
2. Contact My Oracle Support (MOS) for further assistance.

33003 - Insufficient memory for DM-IWF

Alarm Group:
Description: DA-MP does not have sufficient memory to support DM-IWF
Severity: Critical
Instance: Default
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDmiwfAppInsufficientMemoryFailureNotify
Recovery:
1. If the VM:Database DA-MP profile is applied to the DA-MP (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, contact My Oracle Support (MOS) for further assistance on how to upgrade memory.

33004 - DM-IWF Transaction Response Queue Utilization

Alarm Group: DIWF
Description: The DM-IWF Transaction Response Queue Utilization is approaching its maximum engineered capacity.
Severity: Minor, Major, Critical
Instance: RxDmiwfTranRspMsgQueue, DM-IWF
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDmiwfAppTransactionResponseQueueUtilizationNotify
Recovery:
1. This alarm should not normally occur when no other congestion alarms are asserted. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that
is preventing it from processing message from its transaction response queue. Examine the Alarm log in **Alarms & Events**.

2. Contact **My Oracle Support (MOS)** for assistance.

### 33005 - DM-IWF PTR Pool Utilization

**Alarm Group:** DIWF  
**Description:** The DM-IWF PTR Pool Utilization is approaching its maximum engineered capacity. DM-IWF allocates a pending transaction record (PTR) for every pending Diameter-to-MAP and MAP-to-Diameter transaction. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.  
**Severity:** Minor, Major, Critical  
**Instance:** Default  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** eagleXgDiameterDmiwfAppPTRPoolUtilizationNotify  
**Recovery:**  
1. Examine the Alarm log in **Alarms & Events** a evaluate whether the DSR Application Task might be experiencing a problem processing the messages. The rate of messages being processed by DM-IWF can be monitored from the from **Status & Manage > KPIs** page  
2. If one or more DA-MPs in a server site have failed, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DA-MP server status can be monitored from the **Status & Manage > Server**.  
3. If one or more DM-IWF instances configured in a server site are unable to provide service, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DM-IWF application admin state can be monitored from 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, contact **My Oracle Support (MOS)**.

### 33006 - MD-IWF Service Congestion

**Event Group:** DIWF  
**Description:** DM-IWF could not forward a Request to MD-IWF due to MD-IWF Service Congestion  
**Severity:** Info  
**Instance:** <DAMPName>  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**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, 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
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIWFErrorNotify
Recovery:
   If the problem persists, 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 allocation a pending transaction record (PTR) for the transaction. DM-IWF allocates a PTR for every pending Diameter-to-MAP and MAP-to-Diameter transaction. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted
Severity: Info
Instance: <DAMPName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterDmiwfMaxPendTransactionsAllowedExceededNotify
Recovery:
1. Examine the Alarm log in Alarms & Events a evaluate whether the DSR Application Task might be experiencing a problem processing the messages. The rate of messages being processed by DM-IWF can be monitored from the from Status & Manage > KPIs page
2. If one or more DA-MPs in a server site have failed, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DA-MP server status can be monitored from the Status & Manage > Server.
3. If one or more DM-IWF instances configured in a server site are unable to provide service, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DM-IWF application admin state can be monitored from 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, contact My Oracle Support (MOS).

33009 - DM-IWF unexpected Answer response received from a SS7-MP

**Event Group:** DIWF
**Description:** No pending transaction was found for the Answer response received from SS7-MP. When a Request message is forwarded to an SS7-MP, DM-IWF creates a pending transaction record (PTR). The PTR is abandoned if an Answer response is not received in a timely fashion.
**Severity:** Info
**Instance:** <DAMPName>
**HA Score:** Normal
**Auto Clear Seconds:** 0 (zero)
**OID:** eagleXgDiameterDmiwfUnexpectedAnswerRspReceivedFromSS7MPNotify
**Recovery:**
1. If this event is occurring frequently, the MAP Response Timeout may be set too low. The MAP Response Timeout value can be reviewed via Main Menu -> MAP-Diameter IWF -> Configuration -> MD-IWF Options screen.
2. If the problem persists, contact My Oracle Support (MOS).

33010 - MD-IWF ComAgent Connection exhausted

**Event Group:** DIWF
**Description:** DM-IWF failed to receive a Diameter Answer in response to a Diameter Request that was forwarded to MD-IWF Routed Service, in a timely fashion
**Severity:** Info
**Instance:** <DAMPName>
**HA Score:** Normal
**Auto Clear Seconds:** 0 (zero)
**OID:** eagleXgDiameterDmiwfMapComAgentConnectionExhaustedNotify
**Recovery:**
1. If this event is occurring frequently, the MAP Response Timeout may be set too low. The MAP Response Timeout value can be reviewed via Main Menu -> MAP-Diameter IWF -> Configuration -> MD-IWF Options screen.
2. If the problem persists, contact My Oracle Support (MOS).

33011 - DM-IWF Answer Timeout

**Event Group:** DIWF
Description: DM-IWF failed to receive a Diameter Answer in response to a Diameter Request that was forwarded to MD-IWF Routed Service, within the DM-IWF Pending Answer Timer expiration.

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAnswerTimeoutNotify

Recovery:
1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. It’s possible that the MAP Origination Transaction Timer value is set too low. The MAP Origination Transaction Timer value setting can be viewed via the following GUI screen: Main Menu > MAP Interworking > Configuration > Options (MD-IWF tab).
2. If the problem persists, contact My Oracle Support (MOS).

33012 - DM-IWF encode decode error

Event Group: DIWF

Description: The decoder has reported an error causing the Request to be discarded.

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfDecodeErrorNotify

Recovery:
If the problem persists, contact My Oracle Support (MOS).

33013 - DRL queue exhaustion

Event Group: DIWF

Description: DM-IWF failed to forward a Diameter message to DRL due to DRL queue exhaustion

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDrlQueueExhaustionNotify

Recovery:
Note: This alarm should not occur unless the MP is experiencing local congestion as indicated by 22200 - Local MP Congestion, 22201 - Ingress Message Rate, 22204 - Request Message Queue Utilization, and 22205 - Answer Message Queue Utilization.

If the problem persists, contact My Oracle Support (MOS).

33014 - Incompatible DA-MP Profile for DM-IWF

Alarm Group: DIWF
Description: DA-MP has been assigned a profile that is incompatible with DM-IWF
Severity: Critical
Instance: Default
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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, contact My Oracle Support (MOS) for further assistance.

33015 - DM-IWF Diameter message size exceeded maximum supported size

Event Group: DIWF
Description: DM-IWF failed to forward the Diameter message to SS7-MP because the message size exceeds supported maximum message size
Severity: Info
Instance: <DAMPName>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterDmiwfMaxDiameterMsgSizeExceededNotify
Recovery:

Occurrence of this event indicates that diameter message received has size that exceeds maximum diameter message size supported by MAP-Diameter Interworking function and therefore be handled as "Internal Processing Error". Source of these requests can be tracked using "Origin Host", "Application Id" and "Command Code".

MD-IWF (33050-33099)

This section provides information and recovery procedures for MD-IWF alarms and events, ranging from 33050 to 33099, and lists the type of alarms and events that can occur on the system.

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

33050 - MD-IWF Ingress Message Rate

Alarm Group: MIWF

Description: The ingress message rate for the MD-IWF Application is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfIngressMsgRateNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via Main Menu > Diameter > Configuration > Application Routing Rules.

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. Contact My Oracle Support (MOS) for further assistance.

33051 - MD-IWF Application Degraded or Unavailable

Alarm Group: MIWF

Description: MD-IWF Application operational status is Degraded or Unavailable.

Severity: Major, Critical

Instance: Default
HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfApplDegradedOrUnavailableNotify

Recovery:
1. An MD-IWF Application operational status becomes Degraded when either the Admin State is set to disabled with the forced shutdown option or the Admin State is set to disabled with the graceful shutdown option and the graceful shutdown timer expires.

2. The MD-IWF Application can also become Degraded when it reaches Congestion Level 1, 2, or 3 if enabled.
   
   **Note:** This alarm will NOT be raised when the MD-IWF application is shutting down gracefully or application is in Disabled state. Only the MD-IWF Application operational status will be changed to Unavailable.

3. An MD-IWF Application operational status becomes Unavailable when either the Admin State is set to disabled with the forced shutdown option or the Admin State is set to disabled with the graceful shutdown option and the graceful shutdown timer expires.

4. The MD-IWF Application can also become Unavailable when it is isolated from the SS7 network.
   
   **Note:** This alarm will NOT be raised when the MD-IWF application is shutting down gracefully or application is in Disabled state. Only the MD-IWF Application operational status will be changed to Unavailable.

5. Monitor the MD-IWF Application status can be monitored from **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, contact **My Oracle Support (MOS)**.

**33052 - MD-IWF Notified that DM-IWF Service Status is Down**

Alarm Group: MIWF

Description: The MD-IWF is notified via ComAgent that the rolled-up DM-IWF Service Status is Down.

Severity: Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfUserSvcDownNotify

Recovery:
1. Investigate the status of all DA-MP servers. As this status is a rolled-up status, it indicates that no DA-MP servers are able to be a provider of the DM-IWF ComAgent Routed Service.

2. Contact **My Oracle Support (MOS)** for further assistance.
33053 - MD-IWF DiamTrans Task Queue Utilization

Alarm Group: MIWF

Description: The MD-IWF Application DiamTrans Task Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxMdIwfDiamTransMsgQueue (TaskID), MD-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamTransQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via Main Menu > Diameter > Configuration > Application Routing Rules.

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. Contact My Oracle Support (MOS) for further assistance.

33054 - MD-IWF MapTrans Task Queue Utilization

Alarm Group: MIWF

Description: The MD-IWF Application MapTrans Task Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxMdIwfMapTransMsgQueue (TaskId), MD-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfMapTransQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via Main Menu > Diameter > Configuration > Application Routing Rules.

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. 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 Routing Rules.  
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. 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:** 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:

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. Contact My Oracle Support (MOS) for further assistance.

33059 - MD-IWF MapToDiam PTR Utilization

Alarm Group: MIWF
Description: MD-IWF Application MapToDiam PTR Utilization is approaching its maximum engineered capacity.
Severity: Minor, Major, Critical
Instance: None
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfMapToDiamPtrUtilNotify
Recovery:
1. A MapToDiam PTR is allocated for every pending MAP-to-Diameter transaction. The size of the PTR size is engineered based on an average transaction holding size. If the PTRs become depleted, no new transactions can be processed by the MD-IWF application.

2. Determine if there are long delays in the Diameter or SS7 networks. PTR pool exhaustion can be reduced or eliminated by reducing the MAP timer values.

3. The current MAP timers can be viewed in the GUI at Main Menu > MAP Interworking > Configuration > MD-IWF Options.

4. Contact My Oracle Support (MOS) for further assistance.

33060 - SS7-MP Profile Not Assigned
   
   **Alarm Group:** MIWF  
   **Description:** An SS7-MP configuration profile has not been assigned to this SS7-MP  
   **Severity:** Critical  
   **Instance:** Default  
   **HA Score:** Normal  
   **Auto Clear Seconds:** 0 (zero)  
   **OID:** eagleXgDiameterSs7MpProfileNotAssignedNotify  

   **Recovery:**  
   1. If the SS7-MP has been assigned an MP Profile from an SO GUI 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, contact My Oracle Support (MOS) for further assistance.

33062 - Insufficient Memory for MD-IWF
   
   **Alarm Group:** MIWF  
   **Description:** SS7-MP does not have sufficient memory to support MD-IWF  
   **Severity:** Critical  
   **Instance:** None  
   **HA Score:** Normal  
   **Auto Clear Seconds:** 0 (zero)  
   **OID:** eagleXgDiameterMdIwfInsufficientMemoryForMdiwfNotify  

   **Recovery:**  
   1. If MD-IWF was mistakenly activated, deactivate MD-IWF.  
   2. If the SS7-MP does not have sufficient physical memory, upgrade the memory.  
   3. Contact My Oracle Support (MOS) for further assistance.
33063 - MD-IWF SS7-MP not associated with a Place

Alarm Group: MIWF
Description: SS7-MP does not have sufficient memory to support MD-IWF
Severity: Critical
Instance: Default
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfSs7MpNotAssocWithPlaceNotify

Recovery:
1. Set the MD-IWF admin state to Disabled on the SS7-MP Server.
2. If the Server is not associated with an AppWorks place, add the Server to an appropriate AppWorks Place. Then set the MD-IWF admin state to Enabled on the SS7-MP Server.
3. Contact My Oracle Support (MOS) for further assistance.

33065 - MD-IWF Resource Exhaustion

Event Group: MIWF
Description: MD-IWF Application is unable to process a message due to resource exhaustion.
Severity: Info
Instance: None
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfResourceExhaustionNotify

Recovery:
1. Check to see if any of the following resource utilization alarms are present on the SS7-MP. If so, follow the steps specified for the given alarm.
   - 33053 - MD-IWF DiamTrans Task Queue Utilization
   - 33054 - MD-IWF MapTrans Task Queue Utilization
   - 33055 - MD-IWF DAMPInterface Task Queue Utilization
   - 33058 - MD-IWF DiamToMap PTR Utilization
   - 33059 - MD-IWF MapToDiam PTR Utilization
   - 22202 - PDU Buffer Pool Utilization
2. Contact My Oracle Support (MOS) for assistance if needed.

33066 - MD-IWF orphan Diameter Answer message received

Event Group: MIWF
**Description:** MD-IWF Application received a Diameter Answer message for which no Pending Transaction record exists.

**Severity:** Info

**Instance:** mapiwf

**HA Score:** Normal

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

**OID:** eagleXgDiameterMdIwfOrphanDiamAnswerNotify

**Recovery:**

1. When MD-IWF sends a Diameter Request message to a DA-MP, it allocates a PTR and starts a timer (value is user configurable). The pending transaction is abandoned if a Diameter Answer response is not received within the user-configurable time limit. If this event is occurring frequently, the timer may be set too low. The Diameter Response Timeout value can be viewed via the Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options NO GUI Screen.

2. Contact *My Oracle Support (MOS)* for assistance if needed.

**33067 - MD-IWF orphan MAP Response message received**

**Event Group:** MIWF

**Description:** MD-IWF Application received a MAP response message for which no Pending Transaction record exists.

**Severity:** Info

**Instance:** mapiwf

**HA Score:** Normal

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

**OID:** eagleXgDiameterMdIwfOrphanMapResponseNotify

**Recovery:**

1. If this event is occurring frequently, the configurable MAP Response timer may be set too low. The MAP Response Timeout value can be viewed via the NO GUI Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options.

2. Contact *My Oracle Support (MOS)* for assistance if needed.

**33068 - MD-IWF MAP Response timeout**

**Event Group:** MIWF

**Description:** MD-IWF Application sent a MAP request message to the SS7 network, but timed out waiting for the MAP response.

**Severity:** Info

**Instance:** mapiwf

**HA Score:** Normal
Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfMapResponseTimeoutNotify

Recovery:

1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. It is possible that the MAP Response Timeout value is set too low.
2. The configured MAP Response Timeout value can be viewed via Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options.
3. Contact My Oracle Support (MOS) for assistance if needed.

33069 - MD-IWF Diameter Answer timeout

Event Group: MIWF

Description: MD-IWF Application sent a Diameter Request message to the DA-MP, but timed out waiting for the Diameter Answer.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamAnswerTimeoutNotify

Recovery:

1. MAP-to-Diameter timeouts could be caused by delays in the Diameter network. It is possible that the Diameter Response Timeout value is set too low.
2. The configured Diameter Response Timeout value can be viewed via the NO GUI Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options.
3. Contact My Oracle Support (MOS) for assistance if needed.

33070 - MD-IWF Generated Diameter Answer error message due to Diameter Exception

Event Group: MIWF

Description: An error occurred while MD-IWF Application was processing a Diameter Request message, causing it generate a Diameter Answer error message.

Severity: Info

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfGeneratedDiamErrorAnswerNotify

Recovery:

Contact My Oracle Support (MOS) if assistance is needed.
33071 - MD-IWF Generated MAP Error Response due to MAP exception

Event Group: MIWF
Description: An error occurred while MD-IWF Application was processing a MAP request message, causing it generate a MAP response error message.
Severity: Info
Instance: mapiwf
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfGeneratedMapErrorResponseNotify
Recovery:
Contact My Oracle Support (MOS) if assistance is needed.

33072 - MD-IWF received TCAP Notice from SS7 network

Event Group: MIWF
Description: MD-IWF Application received a TCAP Notice from the SS7 network.
Severity: Info
Instance: mapiwf
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: 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

Event Group: MIWF
Description: MD-IWF Application admin state was changed to Enabled on the SS7-MP
Severity: Info
Instance: mapiwf
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfAdminStateChangedNotify
Recovery:
No action required.

33074 - MD-IWF admin state set to Disabled

event Group: MIWF

description: MD-IWF Application admin state was changed to Disabled on the SS7-MP

severity: Info

instance: mapiwf

ha score: Normal

auto clear seconds: 0 (zero)

oid: eagleXgDiameterMdIwfAdminStateDisabledNotify

recovery:

no action required.

33075 - MD-IWF received ComAgent error or DM-IWF NACK

event Group: MIWF

description: MD-IWF sent a Diameter Request message to DM-IWF that resulted in a ComAgent error / timeout or in a DM-IWF NACK.

severity: Info

instance: mapiwf

ha score: Normal

auto clear seconds: 0 (zero)

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

auto clear seconds: 0 (zero)

oid: eagleXgDiameterMdIwfDiamAnsRcvdFrmUnexcpDaMpNotify

recovery:
This error is not expected to occur. 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

Auto Clear Seconds: 0 (zero)

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. 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

Event Group: MIWF

Description: MD-IWF Application received a Diameter EIR message but the Destination-Host AVP was either 1) not present or 2) the Destination-Host AVP value was not present in table DiamIdentityGta.

Severity: Info

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamEirRecdDestHostNotPresentNotify

Recovery:

1. For case 1, investigate why the Destination-Host AVP was not present in the message. The DSR expects this AVP to be present.
2. For case 2, check to see if table DiamIdentityGta is configured correctly. It is possible the given Destination Host should be present in this table. This table is configured on the NO GUI via Main Menu > MAP-Diameter IWF > Configuration > Diameter Identity GTA.
3. Contact My Oracle Support (MOS) for assistance if needed.
33079 - MD-IWF message translation failed

Event Group: MIWF
Description: MD-IWF attempt to perform message translation was unsuccessful.
Severity: Info
Instance: mapiwf
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfMessageTranslationFailedNotify

Recovery:
1. Based on the Translation Error Details, examine the message being translated and attempt to identify the reason for the failure
2. Contact My Oracle Support (MOS) for assistance if needed.

33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message

Event Group: MIWF
Description: EDL failure occurred while MD-IWF attempted to encode a Diameter message.
Severity: Info
Instance: mapiwf
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterMdIwfDiamEirRecdDestHostNotPresentNotify

Recovery:
1. Examine the EDL error text in order to determine the reason for failure. If the encode failure is due to exceeding the maximum supported Diameter message size, and this event is being raised frequently, then it may be necessary to increase the engineering configurable parameter (DiameterMaxMessageSize in table MapIwfLongConfig) for maximum Diameter message size.
2. 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

- **Event Group:** GLA
- **Description:** Message received was rejected because of a decoding failure
- **Severity:** Info
- **Instance:** "MP"
- **HA Score:** Normal
- **Throttle Seconds:** 60
- **OID:** eagleXgDiameterGlaMessageDecodingFailureNotify

**Recovery:**
1. While parsing the message, one of the following conditions occurred:
   - The message content was inconsistent with the "Message Length" in the message header.
   - The IMSI contained in the User-Name AVP was considered invalid due to length.
   - The MSISDN contained in the MSISDN AVP was considered invalid due to length.
2. These protocol errors can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node. Collect a trace containing the GGR, and determine which node is causing the invalid data.
3. If the problem persists, contact *My Oracle Support (MOS)*.

33101 - GLA Incorrect Application ID or Command Code

- **Event Group:** GLA
- **Description:** Message received was rejected because the Application ID was not GL (16777321) or the Command Code was not GGR (8388655).
- **Severity:** Info
- **Instance:** "MP"
- **HA Score:** Normal
- **Throttle Seconds:** 60
- **OID:** 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

- **Event Group:** GLA
Description: Message received was rejected because it did not contain and IMSI or an MSISDN in a Subscription-ID AVP
Severity: Info
Instance: "MP"
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterGlaMissingSubscriberIdNotify
Recovery:
1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.
2. If this condition is met, inspect each element between the GQC and GWS to determine if Subscriber information within the Request is being modified.

33103 - GLA Communication Agent Error
Event Group: GLA
Description: GLA was unable to communicate with the pSBR-Binding due to a communications error
Severity: Info
Instance: "MP"
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterGlaComAgentErrorNotify
Recovery:
1. Examine the current state of the pSBR-B via the Communication Agent > Maintenance > HA Service Status screen.
2. Examine the status of the Reporting Server’s BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persist, contact My Oracle Support (MOS).

33104 - GLA Duplicate Subscriber ID
Event Group: GLA
Description: Message received was rejected because it contained both a User-Name AVP and a MSISDN AVP
Severity: Info
Instance: "MP"
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterGlaDuplicateSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.
2. Inspect each element between 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

Event Group: GLA
Description: Message could not be routed because the internal "Answer Message Queue" to the DSR Relay Agent was full.
Severity: Info
Instance: "MP"
HA Score: Normal
Throttle Seconds: 60

OID: eagleXgDiameterGlaRoutingAttemptFailureDrlQueueExhNotify
Recovery:

1. This condition should not occur unless the DSR is experiencing severe congestion due to excessive traffic levels arriving on the DRL Answer Queue.
2. GL traffic should be diverted from the DA-MP to other DA-MPs in the DSR, or to another DSR.

33106 - GLA Communication Agent Timeout

Event Group: GLA
Description: GLA was unable to communicate with the pSBR-Binding and the query timed out.
Severity: Info
Instance: "MP"
HA Score: Normal
Throttle Seconds: 60

OID: eagleXgDiameterGlaComAgentTimeoutNotify
Recovery:

1. Examine the current state of the pSBR-B via the Communication Agent > Maintenance > HA Service Status screen.
2. Examine the status of the Reporting Server’s BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, 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, contact My Oracle Support (MOS) for assistance.

33121 - GLA pSBR-B Response Task Message Queue Utilization

Alarm Group: GLA

Description: GLA’s pSBR-B Response Message Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxGlaResponseMsgQueue, GLA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterGlaRespTaskMessageQueueUtilizationNotify

Recovery

1. Determine if the GLA pSBR Response Task is mis-configured (Eg. 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, contact *My Oracle Support (MOS)* for additional assistance.
Chapter 4

Key Performance Indicators (KPIs)

This section provides general information about KPIs, and lists the KPIs that can appear on the Status & Manage KPIs GUI page.

Topics:

- General KPIs information.....360
- Computer Aided Policy Making (CAPM) KPIs.....363
- Charging Proxy Application (CPA) KPIs.....363
- Communication Agent (ComAgent) KPIs.....364
- Connection Maintenance KPIs.....364
- Diameter (DIAM) KPIs.....364
- DM-IWF KPIs.....365
- GLA KPIs.....366
- IDIH KPIs.....366
- IP Front End (IPFE) KPIs.....366
- MD-IWF KPIs.....367
- Message Processor (MP) KPIs.....367
- Full Address Based Resolution (FABR) KPIs...368
- Policy Diameter Routing Agent (PDRA) KPIs.....369
- Policy SBR (pSBR) KPIs.....369
- Range Based Address Resolution (RBAR) KPIs.....370
- Session Binding Repository (SBR) KPIs.....370
- SS7/Sigtran KPIs.....371
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 the user 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 Unk for "Unknown".

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 NOAMP server or an SOAM server.

KPIs server elements

This table describes KPIs that appear regardless of server role.

Table 11: KPIs Server Elements

<table>
<thead>
<tr>
<th>KPIs Status Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Element</td>
<td>The network element name (set up on the Configuration &gt; Network Elements page) associated with each Server Hostname.</td>
</tr>
<tr>
<td>Server Hostname</td>
<td>The server hostname set up on the Configuration &gt; Servers page. All servers in the system are listed here.</td>
</tr>
<tr>
<td>Server Indicators:</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Percentage utilization of all processors on the server by all software as measured by the operating system.</td>
</tr>
<tr>
<td>KPIs Status Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>RAM</td>
<td>Percentage utilization of physical memory on the server by all software as measured by TPD.</td>
</tr>
<tr>
<td>Swap</td>
<td>Percentage utilization of swap space on the server by all software as measured by TPD.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The total amount of time the server has been running.</td>
</tr>
</tbody>
</table>

**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 to select an application tab to see KPI data relevant to the application.

   **Note:** The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server. Collection of KPI data is handled solely by NOAMP servers in systems that do not support SOAMs.

**KPIs data export elements**

This table describes the elements on the **KPIs Export** page.

**Table 12: Schedule KPI Data Export Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
</table>
| Export Frequency   | Frequency at which the export occurs | Format: Radio button  
Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily  
Default: Once |
| Task Name          | Name of the scheduled task          | Format: Textbox  
Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-).  
Task Name must begin and end with an alphanumeric character. |
| Description        | Description of the scheduled task   | Format: Textbox  
Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). |
### 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 Displaying 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 13: CAPM KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing time [ms]</td>
<td>Average processing time of Rule Template on a per Rule Template basis.</td>
</tr>
<tr>
<td>Active Templates</td>
<td>Number of Rule Templates that are in Active state.</td>
</tr>
<tr>
<td>Test Templates</td>
<td>Number of Rule Templates that are in Test state.</td>
</tr>
<tr>
<td>Development Templates</td>
<td>Number of Rule Templates that are in Development state.</td>
</tr>
</tbody>
</table>

Charging Proxy Application (CPA) KPIs

The KPI values associated with CPA are visible using Main Menu > Status & Manage > KPIs.

Table 14: Charging Proxy Application (CPA) KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPA Answer Message Rate</td>
<td>Track the average number of Answer messages processed per second by the CPA application.</td>
</tr>
<tr>
<td>CPA Ingress Message Rate</td>
<td>Track the average number of Diameter messages received per second by the CPA application.</td>
</tr>
<tr>
<td>CPA Request Message Rate</td>
<td>Track the average number of Request messages processed per second by the CPA application.</td>
</tr>
</tbody>
</table>
Key Performance Indicators (KPIs)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cSBR Query Error Rate</td>
<td>Track the average number of errors received per second by the CPA application when attempting to query (read, create, update, delete) SBR.</td>
</tr>
<tr>
<td>cSBR Query Rate</td>
<td>Track the average number of SBR Queries sent per second by the CPA application.</td>
</tr>
</tbody>
</table>

Communication Agent (ComAgent) KPIs

The KPI values associated with ComAgent are available using **Main Menu > Status & Manage > KPIs**.

**Table 15: Communication Agent KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Data Ingress message rate</td>
<td>Average of User Data Ingress Message Rate (messages per second) utilization on a MP server. The Ingress Message Rate is the number of User Data StackEvents (messages) that ComAgent delivers to Application Layers Queue.</td>
</tr>
</tbody>
</table>

Connection Maintenance KPIs

The KPI values associated with Connection Maintenance are available using **Main Menu > Status & Manage > KPIs**.

**Table 16: Connection Maintenance KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxConnAvgMPS</td>
<td>Exponentially smoothed average rate in MPS on the connection. Note: This measurement will be sampled periodically and reported in the Connections Maintenance GUI as a type of KPI.</td>
</tr>
</tbody>
</table>

Diameter (DIAM) KPIs

The KPI values associated with Diameter are available using **Main Menu > Status & Manage > KPIs**.
Table 17: DIAM KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Trans Success Rate</td>
<td>Percentage of ingress peer-to-peer transactions successfully complete</td>
</tr>
<tr>
<td>MsgCopyTxQueueUtilization</td>
<td>Percentage of utilization of the Message Copy Tx Queue</td>
</tr>
<tr>
<td>Avg Rsp Time (ms)</td>
<td>Average time from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer</td>
</tr>
<tr>
<td>Routing Success Rate</td>
<td>Percentage of transactions successfully routed on first attempt</td>
</tr>
<tr>
<td>Avg Diameter Process CPU Util</td>
<td>Average percent Diameter process CPU utilization (0-100%) on an MP server</td>
</tr>
<tr>
<td>Avg IMR Offered</td>
<td>Average Ingress Offered message rate (messages per second) on a MP server. Offered message rate is number of ingress Diameter messages before any Ingress controls are applied</td>
</tr>
<tr>
<td>Avg IMR Accepted</td>
<td>Average Ingress Accepted message rate (messages per second) on a MP server. Accepted message rate is number of routable messages accepted by MP after all Ingress controls are applied</td>
</tr>
<tr>
<td>Avg Message Processing Load</td>
<td>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 Reroutes and Msgcopy</td>
</tr>
</tbody>
</table>

DM-IWF KPIs

The KPI values associated with DM-IWF are visible using Main Menu > Status & Manage > KPIs

Table 18: DM-IWF KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Msg Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Diameter-to-MAP Trans Msg Rate</td>
<td>Average number of Diameter-to-MAP transaction messages processed per second.</td>
</tr>
</tbody>
</table>
### Key Performance Indicators (KPIs)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP-to-Diameter Trans Msg Rate</td>
<td>Average number of MAP-to-Diameter transaction messages processed per second.</td>
</tr>
</tbody>
</table>

#### GLA KPIs

The KPI values associated with GLA are visible using **Main Menu > Status & Manage > KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Message Rate</td>
<td>Average Ingress Message Rate (messages per second) utilization on an MP server for this DSR Application. The Ingress Message Rate is the number of ingress Diameter messages that are selected for processing by the ART and sent to the DSR Application for processing.</td>
</tr>
<tr>
<td>Success Message Rate</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### IDIH KPIs

The KPI values associated with the IDIH will be visible via the GUI **Main Menu > Status & Manage > KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR-DIH TTR Bandwidth (KB/sec)</td>
<td>Average bandwidth used by DSR in sending TTRs (including trace start and stop messages) to DIH in Kbytes per second</td>
</tr>
</tbody>
</table>

#### IP Front End (IPFE) KPIs

The KPI values associated with IPFE are visible using **Main Menu > Status & Manage > KPIs.**

**Table 19: IPFE KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU %</td>
<td>Total CPU used by the IPFE process</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory Total</td>
<td>Absolute memory used by the IPFE process</td>
</tr>
<tr>
<td>Memory %</td>
<td>Percent memory used by the IPFE process</td>
</tr>
<tr>
<td>Mem. Heap</td>
<td>Total heap allocated by the IPFE process</td>
</tr>
<tr>
<td>IPFE Packets/Sec</td>
<td>The average number of packets per second the IPFE receives</td>
</tr>
<tr>
<td>IPFE MBytes/Sec</td>
<td>The average number of megabytes per second the IPFE receives</td>
</tr>
</tbody>
</table>

**MD-IWF KPIs**

The KPI values associated with MD-IWF are visible using **Main Menu > Status & Manage > KPIs**.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Message Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Diameter-to-MAP Ingress Msg Rate</td>
<td>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.</td>
</tr>
<tr>
<td>MAP-to-Diameter Ingress Msg Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Diameter Ingress Message Rate</td>
<td>Average number of Diameter messages (both Requests and Answers) received per second from DA-MPs.</td>
</tr>
<tr>
<td>MAP Ingress Message Rate</td>
<td>Average number of MAP messages (both requests and responses) received per second from SS7 network.</td>
</tr>
</tbody>
</table>

**Message Processor (MP) KPIs**

The KPI values associated with MP are available using **Main Menu > Status & Manage > KPIs**.
Table 20: MP KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg Diameter Process CPU Util</td>
<td>Average percent Diameter Process CPU utilization (0-100%) on a MP server.</td>
</tr>
<tr>
<td>Avg IMR Offered</td>
<td>Average Ingress Offered message rate (messages per second) on a MP server.</td>
</tr>
<tr>
<td>Avg IMR Accepted</td>
<td>Average Ingress Accepted message rate (messages per second) on a MP server.</td>
</tr>
<tr>
<td>Avg Messsage Processing Load</td>
<td>Average message processing load (messages per second) on a MP server.</td>
</tr>
</tbody>
</table>

Full Address Based Resolution (FABR) KPIs

The KPI values associated with FABRr are available using **Main Menu > Status & Manage > KPIs.**

Table 21: FABR KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Message Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Resolved Message Rate</td>
<td>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.</td>
</tr>
<tr>
<td>DP Response Time Average</td>
<td>Average DP response time is the average time (in milliseconds) it takes to receive a DP response after sending the corresponding DP query.</td>
</tr>
</tbody>
</table>
Key Performance Indicators (KPIs)

Policy Diameter Routing Agent (PDRA) KPIs

The KPI values associated with PDRA are available using Main Menu > Status & Manage > KPIs.

Table 22: P-DRA KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-DRA Ingress Message Rate</td>
<td>This KPI is to measure the average number of Diameter messages per second including both requests and answers received by P-DRA from the DRL layer.</td>
</tr>
</tbody>
</table>

Policy SBR (pSBR) KPIs

The KPI values for pSBR are visible using Main Menu > Status & Manage > KPIs.

Table 23: pSBR KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSBR memory utilization</td>
<td>pSBR memory utilization (0-100%)</td>
</tr>
<tr>
<td>pSBR process CPU utilization</td>
<td>pSBR Process CPU Percent Utilization</td>
</tr>
</tbody>
</table>

Table 24: pSBR-Binding KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSBR Bindings</td>
<td>Total Number of Active Bindings</td>
</tr>
<tr>
<td>pSBR Avg Binding DB Read Rate</td>
<td>Average number of binding DB reads per second</td>
</tr>
<tr>
<td>pSBR Avg Binding DB Write Rate</td>
<td>Average number of binding DB writes per second</td>
</tr>
</tbody>
</table>

Note: In order to view the current number of subscribers with a binding for the entire P-DRA network, an appropriate scope must be chosen on the KPI screen. Valid scopes must encompass all binding pSBR servers as follows: Entire Network, filtered by Resource Domain with the Policy Binding resource domain selected, or filtered by Place Association with the Policy DRA Binding Region place association selected.

Table 25: pSBR-Session KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pSBR Sessions</td>
<td>Total Number of Active Sessions</td>
</tr>
<tr>
<td>pSBR Avg Session DB Read Rate</td>
<td>Average number of session DB reads per second</td>
</tr>
</tbody>
</table>
### Range Based Address Resolution (RBAR) KPIs

The KPI values associated with RBAR are available using Main Menu > Status & Manage > KPIs.

Table 26: RBAR KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg Resolved Message Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Ingress Message Rate</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Session Binding Repository (SBR) KPIs

The KPI values associated with SBR are visible using Main Menu > Status & Manage > KPIs.

Note: SBR KPIs are only associated with the CPA function.

Table 27: SBR KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current session bindings</td>
<td>Current number of session bindings</td>
</tr>
<tr>
<td>Mostly Stale session bindings</td>
<td>Number of session bindings found to be Mostly Stale during the previous audit</td>
</tr>
<tr>
<td>Session binding capacity</td>
<td>Number of session bindings as a percentage of the total capacity</td>
</tr>
<tr>
<td>Load Shed Rate</td>
<td>Rate (per second) at which queries (read, create, update, delete) are being shed due to congestion</td>
</tr>
<tr>
<td>Time to process query</td>
<td>Lifetime of a transaction in microseconds (time between query received and response sent)</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Query rate</td>
<td>Number of queries (read, create, update, delete) processed per second</td>
</tr>
</tbody>
</table>

### SS7/Sigtran KPIs

#### Table 28: SS7/Sigtran KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCP Xmit Msgs/Sec</td>
<td>SCCP messages transmitted per second</td>
</tr>
<tr>
<td>SCCP Recv Msgs/Sec</td>
<td>SCCP messages received per second</td>
</tr>
<tr>
<td>SS7 Process CPU Utilization</td>
<td>The average percent of SS7 Process CPU utilization on an MP server.</td>
</tr>
<tr>
<td>Ingress Message Rate</td>
<td>The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue.</td>
</tr>
<tr>
<td>M3RL Xmit Msgs/Sec</td>
<td>M3RL DATA MSUs/Sec sent.</td>
</tr>
<tr>
<td>M3RL Recv Msgs/Sec</td>
<td>M3RL DATA MSUs/Sec received.</td>
</tr>
</tbody>
</table>
### Chapter 5

**Measurements**

**Topics:**

- General measurements information.....375
- Address Resolution Exception measurements..379
- Address Resolution Performance measurements.....388
- Application Routing Rules measurements.....396
- Association Exception measurements.....399
- Association Performance measurements.....408
- Association Usage measurements.....410
- Charging Proxy Application (CPA) Exception measurements.....413
- Charging Proxy Application (CPA) Performance measurements.....418
- Charging Proxy Application (CPA) Session DB measurements.....425
- Communication Agent (ComAgent) Exception measurements.....431
- Communication Agent (ComAgent) Performance measurements.....459
- Computer Aided Policy Making (CAPM) measurements.....476
- Connection Congestion measurements.....479
- Connection Exception measurements.....487
- Connection Performance measurements.....495
- Diameter Signaling Router (DSR) Application Exception measurements.....507
- Diameter Signaling Router (DSR) Application Performance measurements.....515
- Diameter Egress Transaction measurements....535
- Diameter Exception measurements.....539
- Diameter Ingress Transaction Exception measurements.....566

This section provides general information about measurements (including measurement procedures), and lists the measurements that display on measurement reports.
• Diameter Ingress Transaction Performance measurements.....583
• Diameter Performance measurements.....588
• Diameter Rerouting measurements.....619
• DM-IWF Exception measurements.....623
• DM-IWF Performance measurements.....629
• Egress Throttle Group Performance measurements.....637
• Full Address Based Resolution (FABR) Application Exception measurements.....645
• Full Address Based Resolution (FABR) Application Performance measurements.....653
• GLA Exception measurements.....663
• GLA Performance measurements.....665
• IDIH measurements.....667
• IP Front End (IPFE) Exception measurements.....669
• IP Front End (IPFE) Performance measurements.....672
• MD-IWF Exception Measurements.....679
• MD-IWF Performance measurements.....688
• MD-IWF SS7 Performance measurements.....704
• MD-IWF Diam Performance Measurements...706
• Message Copy measurements.....708
• Message Priority measurements.....715
• Message Processor (MP) Performance measurements.....721
• OAM.ALARM measurements.....744
• OAM.PERF Measurements.....745
• OAM.SYSTEM measurements.....746
• P-DRA Diameter Usage measurements.....748
• P-DRA Diameter Exception measurements.....760
• P-DRA Congestion Exception measurements..769
• pSBR Binding Performance measurements.....772
• pSBR Session Performance measurements.....780
• pSBR Binding Exception measurements.....785
• pSBR Session Exception measurements.....789
• pSBR Audit measurements.....792
• Peer Node Performance measurements.....802
• Peer Routing Rules measurements.....803
• Route List measurements.....807
• Routing Usage measurements.....810
• Server Exception measurements.....812
• Server TCAP Exception measurements.....813
- Server TCAP Performance measurements.....821
- Session Binding Repository (SBR) Exception measurements.....824
- Session Binding Repository (SBR) Performance measurements.....829
- SS7/Sigtran Measurements.....837
- Transport Manager Measurements.....913
- Transport Exception measurements.....936
- Transport Usage measurements.....944
- Transport Performance measurements.....947
- Topology Hiding Performance measurements..954
General measurements information

This section provides general information about measurements, measurement-related GUI elements, and measurement report procedures.

Measurements

The measurements framework allows applications to define, update, and produce reports for various measurements.

- Measurements are ordinary counters that count occurrences of different events within the system, for example, the number of messages received. Measurement counters are also called pegs.
  Additional measurement types provided by the Platform framework are not used in this release.
- Applications simply peg (increment) measurements upon the occurrence of the event that needs to be measured.
- Measurements are collected and merged at the SOAM and NOAM servers as appropriate.
- The GUI allows reports to be generated from measurements.

Measurements that are being pegged locally are collected from shared memory and stored in a disk-backed database table every 5 minutes on all servers in the network. Measurements are collected every 5 minutes on a 5 minute boundary, i.e. at HH:00, HH:05, HH:10, HH:15, and so on. The collection frequency is set to 5 minutes to minimize the loss of measurement data in case of a server failure, and also to minimize the impact of measurements collection on system performance.

All servers in the network (NOAMP, SOAM, and MP servers) store a minimum of 8 hours of local measurements data. More than 5 minutes of local measurements data is retained on each server to minimize loss of measurements data in case of a network connection failure to the server merging measurements.

Measurements data older than the required retention period are deleted by the measurements framework.

Measurements are reported in groups. A measurements report group is a collection of measurement IDs. Each measurement report contains one measurement group. A measurement can be assigned to one or more existing or new measurement groups so that it is included in a measurement report.

Assigning a measurement ID to a report group ensures that when you select a report group the same set of measurements is always included in the measurements report.

Note: Measurements from a server may be missing in a report if the server is down; the server is in overload; something in the Platform merging framework is not working; or the report is generated before data is available from the last collection period (there is a 25 to 30 second lag time in availability).

Measurement elements

This table describes the elements on the Measurements Report page.
### Table 29: Measurements Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Network Elements, Server Groups, Resource Domains, Places and Place Associations for which the measurements report can be run. <strong>Note:</strong> Measurements for SOAM network elements are not available in systems that do not support SOAMs.</td>
<td>Format: Pulldown list&lt;br&gt;Range: Network Elements in the topology; Server Groups in the topology; Resource Domains in the topology; Places in the topology; Place Associations in the topology&lt;br&gt;<strong>Note:</strong> If no selection is made, the default scope is Entire Network. Default: Entire Network</td>
</tr>
<tr>
<td>Report</td>
<td>A selection of reports</td>
<td>Format: Pulldown list&lt;br&gt;Range: Varies depending on application&lt;br&gt;Default: Group</td>
</tr>
<tr>
<td>Column Filter</td>
<td>The characteristics for filtering the column display</td>
<td>Format: Pulldown list&lt;br&gt;Range: Sub-measurement&lt;br&gt;Sub-measurement Ranges:&lt;br&gt;• Like: A pattern-matching distinction for sub-measurement name, for example, 123* matches any sub-measurement that begins with 123.&lt;br&gt;• In: A list-matching distinction for sub-measurement ID, for example, 3,4,6-10 matches only sub-measurements 3, 4, and 6 through 10. Default: None</td>
</tr>
<tr>
<td>Time Range</td>
<td>The interval of time for which the data is being reported, beginning or ending on a specified date.</td>
<td>Format: Pulldown list&lt;br&gt;Range: Days, Hours, Minutes, Seconds&lt;br&gt;Interval Reference Point: Ending, Beginning&lt;br&gt;Default: Days</td>
</tr>
</tbody>
</table>
Generating a measurements report

Use this procedure to generate and view a measurements report.

1. Select **Measurements > Report**.
   
   The **Measurements Report** page appears.

2. Select the **Scope**.
   
   For details about this field, or any field on the **Measurements Report** page, see **Measurement elements**.

3. Select the **Report**.
4. Select the **Interval**.
5. Select the **Time Range**.
6. Select **Beginning** or **Ending** as the **Time Range** interval reference point.
7. Select the **Beginning** or **Ending** date.
8. Click **Go**.

   The report is generated.

   **Note:** Data for the selected scope is displayed in the primary report page. Data for any available sub-scopes are displayed in tabs. For example, if the selected scope is Entire Network, report data for the entire network appears in the primary report page. The individual network entities within the entire network are considered sub-scopes.

9. To view report data for a specific sub-scope, click on the tab for that sub-scope.

   The report data appears.

Measurements data export elements

This table describes the elements on the **Measurements Report Export** page.

**Table 30: Schedule Measurement Data Export Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>Name of the scheduled task</td>
<td>Format: Textbox; Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-); Task Name must begin and end with an alphanumeric character.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the scheduled task</td>
<td>Format: Textbox; Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-); Description must begin with an alphanumeric character.</td>
</tr>
</tbody>
</table>
### Exporting measurements reports

You can schedule periodic exports of data from the **Measurements Report** page. Measurements data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied on the **Measurements Report** 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 save a measurements report to the file management storage area. Use this procedure to schedule a data export task.

1. **Select** **Measurements > Report**.
   
   The **Measurements Report** page appears. For a description of each field, see *Measurement elements*.

2. **Generate** a measurements report.
   
   For information about how to generate a measurements report, see *Generating a measurements report*.

3. **Click** to select the scope or sub-scope measurement report that you want to export.

4. **Click** **Export**.
   
   The measurement report is exported to a CSV file. Click the link at the top of the page to go directly to the **Status & Manage > Files** page. From the **Status & Manage** page, you can view a list of files.
available for download, including the measurements report you exported during this procedure. The Schedule Measurement Log Data Export page appears.

5. Check the Report Groups boxes corresponding to any additional measurement reports to be exported.

   Note: This step is optional, but is available to allow the export of multiple measurement group reports simultaneously.

6. Select the Export Frequency.

   Note: If the selected Export Frequency is Fifteen Minutes or Hourly, specify the Minutes.

7. Enter the Task Name.

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

   Note: Task Name is not an option if Export Frequency equals Once.

8. Select the Time of Day.

   Note: Time of Day is only an option if Export Frequency equals Daily or Weekly.

9. Select the Day of Week.

   Note: Day of Week is only an option if Export Frequency equals Weekly.

10. Click OK or Apply to initiate the data export task.

    The data export task is scheduled. From the Status & Manage > Tasks page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see Displaying the file list.

Address Resolution Exception measurements

The Address Resolution Exception measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the RBAR Application.

Table 31: Address Resolution Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRbarDecodeFailureResol</td>
<td>Number of Request messages rejected due to a message decoding error.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

E53474 Revision 01, July 2014 379
<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRbarInvalidImsiMcc</td>
<td>Number of times an AVP instance present in Diameter request message is rejected due to the MCC contained in the decoded IMSI falls within one of the configured Reserved MCC Ranges</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailAll</td>
<td>Number of Request messages received which did not resolve to a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailCmdcode</td>
<td>Number of Request messages received with an unknown Command Code.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailDbFail</td>
<td>Number of routing attempt failures due to internal database inconsistency failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailImpiMatch</td>
<td>Number of Request messages received with a valid IMPI that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailImpuMatch</td>
<td>Number of Request messages received with a valid IMPU that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailImsiMatch</td>
<td>Number of Request messages received with a valid IMSI that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailIpv4Match</td>
<td>Number of Request messages received with an IPv4 Address that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailIpv6PrefixMatch</td>
<td>Number of Request messages received with an IPv6-Prefix Address that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailMsisdnMatch</td>
<td>Number of Request messages received with a valid MSISDN that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailNoAddrAvps</td>
<td>Number of Request messages received without a Routing Entity Address AVP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolFailNoValidAddr</td>
<td>Number of Request messages received with at least Routing Entity Address AVP.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>AVP but no valid Routing Entity</td>
<td>Addresses were found.</td>
<td></td>
</tr>
<tr>
<td>RxRbarResolFailUnsigned16Match</td>
<td>Number of Request messages received with an UNSIGNED16 value that did not match a provisioned address or address range.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarUnkAppId</td>
<td>Number of Request messages rejected due to an unknown Application ID.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRbarAbandonRequest</td>
<td>Number of Request messages that are abandoned</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxRbarDecodeFailureResol**

- **Measurement Group:** Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of Request messages rejected due to a message decoding error.
- **Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message and does not decode an AVP which extends beyond the length of the message indicated by the Message Length parameter in the message header.

**Measurement Scope:** Server Group

**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.

**RxFabrInvalidImsiMcc**

- **Measurement Group:** Full Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of times an AVP instance present in a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.
- **Collection Interval:** 5 min

**Peg Condition:** Each time a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.

**Measurement Scope:** Server Group
Recovery:

1. Validate the ranges configured in the Reserved MCC Ranges table.
2. Verify that the MCC portion of the decodable IMSI received by RBAR does not fall within the configured Reserved MCC Ranges.
3. If the problem persists, contact My Oracle Support (MOS).

RxRbarResolFailAll

Measurement Group: Address Resolution Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request messages received which did not resolve to a provisioned address or address range.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.
Measurement Scope: Server Group

Recovery:

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.

View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting RBAR > Configuration > Address Resolutions.

RxRbarResolFailCmdcode

Measurement Group: Address Resolution Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request messages received with an unknown Command Code.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message and, after attempting to validate the ordered pair (Application ID and Command Code), the Command Code is unknown. RBAR invokes the routing exception handling procedure assigned to this Application ID and Routing Exception Type.
Measurement Scope: Server Group

Recovery:

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

**RxRbarResolFailDbFail**

- **Measurement Group:** Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Number of routing attempt failures due to internal database inconsistency failure.
- **Collection Interval:** 5 min
- **Peg Condition:** When RBAR receives a Request message and encounters a run-time database inconsistency.
- **Measurement Scope:** Server Group
- **Recovery:**
  If this problem occurs, contact *My Oracle Support (MOS)*.

**RxRbarResolFailImpiMatch**

- **Measurement Group:** Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Number of Request messages received with a valid IMPI that did not match a provisioned address or address range.
- **Collection Interval:** 5 min
- **Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IMPI and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.
- **Measurement Scope:** Server Group
- **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.

**RxRbarResolFailImpuMatch**

- **Measurement Group:** Address Resolution Exception
- **Measurement Type:** Simple
**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Request messages received with a valid IMPU that did not match a provisioned address or address range.

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IMPU and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

**Measurement Scope:** Server Group

**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.**

---

**RxRbarResolFailImsiMatch**

**Measurement Group:** Address Resolution Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Request messages received with a valid IMSI that did not match a provisioned address or address range.

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IMSI and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

**Measurement Scope:** Server Group

**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.**

---

**RxRbarResolFailIpv4Match**

**Measurement Group:** Address Resolution Exception

**Measurement Type:** Simple
**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Request messages received with an IPv4 Address that did not match a provisioned address or address range

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IPv4 Address and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

**Measurement Scope:** Server Group

**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**.

---

**RxRbarResolFailIpv6prefixMatch**

**Measurement Group:** Address Resolution Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Request messages received with an IPv6-Prefix Address that did not match a provisioned address or address range

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IPv6-Prefix Address and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

**Measurement Scope:** Server Group

**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**.

---

**RxRbarResolFailMsisdnMatch**

**Measurement Group:** Address Resolution Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)
Measurements

Description: Number of Request messages received with a valid MSISDN that did not match a provisioned address or address range

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of MSISDN and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

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.

RxRbarResolFailNoAddrAvps

Measurement Group: Address Resolution Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request messages received without a Routing Entity Address AVP.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message, with the number of AVPs searched—as defined by measurement RxRbarAvgAddrAvps for the message—as 0 and hence, a valid Routing Entity address cannot be found using any of the Routing Entity Types assigned to the ordered pair (Application ID and Command Code).

Measurement Scope: Server Group

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.

RxRbarResolFailNoValidAddr

Measurement Group: Address Resolution Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request messages received with at least Routing Entity Address AVP but no valid Routing Entity Addresses were found.
Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message, with the number of AVPs searched—as defined by measurement RxRbarAvgAddrAvps for the message—as > 0 but, a valid Routing Entity address cannot be found using any of the Routing Entity Types assigned to the ordered pair (Application ID and Command Code).

Measurement Scope: Server Group

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**.

RxRbarResolFailUnsigned16Match

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with an UNSIGNED16 value that did not match a provisioned address or address range.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of UNSIGNED16 and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

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**.

RxRbarUnkAppId

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Request messages rejected due to an unknown Application ID.

Collection Interval: 5 min
**Peg Condition:** When a Request message received and the Application ID is not present in the RBAR configuration.

**Measurement Scope:** Server Group

**Recovery:**

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 misprovisioned or the Application ID is not provisioned in the RBAR routing configuration.

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

**TxRbarAbandonRequest**

**Measurement Group:** Address Resolution Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of Request messages that are abandoned

**Collection Interval:** 5 min

**Peg Condition:** Each time the Routing Exception "Abandon Request" is invoked

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**Address Resolution Performance measurements**

The Address Resolution Performance measurement group is a set of measurements that provide performance information that is specific to a RBAR Application. These measurements allow you to determine how many messages are successfully forwarded and received to/from each RBAR Application.

**Table 32: Address Resolution Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRbarAvgMsgSize</td>
<td>Average size of Request message received.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarMsgs</td>
<td>Number of Diameter messages received by Range Based Address Resolution application.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxRbarResolAll</td>
<td>Number of Addresses Successful Resolved to a Destination.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolAllMp</td>
<td>Number of Addresses Successful Resolved to a Destination by the MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolImpi</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IMPI.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolImpu</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IMPU.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolImsi</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IMSI.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolIpv4</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IPv4 Address.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolIpv6prefix</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IPv6-Prefix Address.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolMsisdn</td>
<td>Number of Addresses Successful Resolved with Routing Entity type MSISDN.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolRateAvg</td>
<td>Average Addresses Successfully Resolved per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolRatePeak</td>
<td>Peak Addresses Successfully Resolved per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolSingleAddr</td>
<td>Number of Addresses Successful Resolved with an Individual Address.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarResolUnsigned16</td>
<td>Number of Addresses Successful Resolved with Routing Entity type UNSIGNED16.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRbarFwdDefaultDest</td>
<td>Number of Request message forwarding attempts using a Default Destination.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRbarFwdNochange</td>
<td>Number of Request message forwarding attempts without changing the message.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TxRbarFwdSuccess</td>
<td>Number of Request messages successfully forwarded (all reasons).</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRbarMsgAttempt</td>
<td>Number of Request message forwarding attempts (all reasons).</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxRbarAvgMsgRate**

**Measurement Group:** Address Resolution Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Average size of Request message received.  
**Collection Interval:** 5 min  
**Peg Condition:** Average calculated for each Request message received as defined by measurement `RxRbarMsgs`.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**RxRbarMsgs**

**Measurement Group:** Address Resolution Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request messages received by RBAR.  
**Collection Interval:** 5 min  
**Peg Condition:** When RBAR receives a Request message and determines that the Application ID in the message header is defined in the routing configuration and valid.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**RxRbarResolAll**

**Measurement Group:** Address Resolution Performance  
**Measurement Type:** Simple
**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Addresses Successful Resolved to a Destination.

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

**Measurement Scope:** Server Group

**Recovery:**
- No action required.

**RxRbarResolAllMp**

**Measurement Group:** Address Resolution Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of Addresses Successful Resolved to a Destination by the MP.

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message and successfully resolves its Application ID, Command Code and Routing Entity to a Destination.

**Measurement Scope:** Server Group

**Recovery:**
- No action required.

**RxRbarResolImpi**

**Measurement Group:** Address Resolution Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Addresses Successful Resolved with Routing Entity type IMPI.

**Collection Interval:** 5 min

**Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IMPI and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

**Measurement Scope:** Server Group

**Recovery:**
- No action required.
Measurements

RxRbarResolImpu

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Addresses Successful Resolved with Routing Entity type IMPU.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMPU and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.
Measurement Scope: Server Group
Recovery:
   No action required.

RxRbarResolImsi

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Addresses Successful Resolved with Routing Entity type IMSI.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMSI and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.
Measurement Scope: Server Group
Recovery:
   No action required.

RxRbarResolIpv4

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Addresses Successful Resolved with Routing Entity type IPv4 Address.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message with a Routing Entity type of IPv4 Address and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.
Measurements

**RxRbarResolIpv6prefix**
- **Measurement Group:** Address Resolution Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Number of Addresses Successful Resolved with Routing Entity type IPv6-Prefix Address.
- **Collection Interval:** 5 min
- **Peg Condition:** When RBAR receives a Request message with a Routing Entity type of IPv6-Prefix Address and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

**RxRbarResolMsisdn**
- **Measurement Group:** Address Resolution Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Number of Addresses Successful Resolved with Routing Entity type MSISDN.
- **Collection Interval:** 5 min
- **Peg Condition:** When RBAR receives a Request message with a Routing Entity type of MSISDN and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

**RxRbarResolRateAvg**
- No action required.

**RxRbarResolRatePeak**
- **Measurement Group:** Address Resolution Performance
Measurements

Measurement Type: Max
Measurement Dimension: Single
Description: Peak Addresses Successfully Resolved per second
Collection Interval: 5 min
Peg Condition: At the end of each sample period associated with average successfully resolved message rate, as defined by measurement *RxRbarResolRateAvg*, if the value exceeds the current value for this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: Server Group

Recovery:
No action required.

**RxRbarResolSingleAddr**

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Addresses Successfully Resolved with an Individual Address.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message and uses the Address Exceptions to successfully resolve its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:
No action required.

**RxRbarResolUnsigned16**

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Addresses Successfully Resolved with Routing Entity type UNSIGNED16.
Collection Interval: 5 min
Peg Condition: When RBAR receives a Request message with a Routing Entity type of UNSIGNED16 and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:
No action required.
Measurements

TxRbarFwdDefaultDest

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request message forwarding attempts using a Default Destination.
Collection Interval: 5 min
Peg Condition: Each time the Routing Exception Forward route the message with a user-configurable Default Destination is invoked.
Measurement Scope: Server Group
Recovery: No action required.

TxRbarFwdNoChange

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request message forwarding attempts without changing the message.
Collection Interval: 5 min
Peg Condition: Each time the Routing Exception Forward route the message unchanged is invoked.
Measurement Scope: Server Group
Recovery: No action required.

TxRbarFwdSuccess

Measurement Group: Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request messages successfully forwarded (all reasons).
Collection Interval: 5 min
Peg Condition: Each time the application successfully enqueues a Request message on the DSR Relay Agent’s Request Message Queue.
Measurement Scope: Server Group
Recovery:
If this value is less than measurement \textit{TxRbarMsgAttempt}, then an internal resource error is occurring. Contact \textit{My Oracle Support (MOS)}, if needed.

\textbf{TxRbarMsgAttempt}

\textbf{Measurement Group:} Address Resolution Performance
\textbf{Measurement Type:} Simple
\textbf{Measurement Dimension:} Arrayed (by Diameter Application ID)
\textbf{Description:} Number of Request message forwarding attempts (all reasons).
\textbf{Collection Interval:} 5 min
\textbf{Peg Condition:} Each time the application attempts to enqueue a Request message on the DSR Relay Agent’s Request Message Queue.
\textbf{Measurement Scope:} Server Group
\textbf{Recovery:}
No action required.

\textbf{Application Routing Rules measurements}

The Application Routing Rules measurement group is a set of measurements associated with the usage of Application Routing Rules. These measurements will allow the user to determine which Application Routing Rules are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed.

\textbf{Table 33: Application Routing Rule Measurements}

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxApplRuleSelected</td>
<td>Number of times that an Application Routing Rule was selected to route a Request message</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplRuleFwdFailAll</td>
<td>Number of times that an Application Routing Rule was selected to route a Request message but the message was not successfully routed (all reasons)</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplRuleFwdFailUnavail</td>
<td>Number of times that an Application Routing Rule was selected to route a Request message but the message was not successfully routed because the DSR Application’s</td>
<td>5 min</td>
</tr>
</tbody>
</table>
**RxApplRuleDuplicatePriority**

**Description:** Number of times that the application routing rule was selected for routing a message but another application routing rule had the same priority and was ignored.

**Collection Interval:** 5 min

**RxArtSelected**

**Description:** Number of times that an application routing rule from ART-X was selected for routing a Request message.

**Collection Interval:** 5 min

---

**RxApplRuleSelected**

**Measurement Group:** Application Routing Rules

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Application Routing Rule ID)

**Description:** Number of times that the application routing rule was selected for routing a Request message.

**Collection Interval:** 5 min

**Peg Condition:** When DRL selects an application routing rule for routing a message.

**Measurement Scope:** Server Group

**Recovery:** No action required.

**RxApplRuleFwdFailAll**

**Measurement Group:** Application Routing Rules

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Application Routing Rule ID)

**Description:** Number of times that the application routing rule was selected for routing a Request message and the message was not successfully routed for any reason.

**Collection Interval:** 5 min

**Peg Condition:** When DRL selects an application routing rule to route a Request message and one of the following conditions is met:

- The DSR Application’s Operational Status is “Unavailable”.
- The DSR Application’s Operational Status is not “Unavailable” but the attempt to enqueue the message to the DSR Application failed.
**RxApplRuleFwdFailUnavail**

- **Measurement Group:** Application Routing Rules
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Application Routing Rule ID)
- **Description:** Number of times that the application routing rule was selected for routing a Request message and the message was not successfully routed because DSR Application’s Operational Status was “Unavailable”.
- **Collection Interval:** 5 min
- **Peg Condition:** When DRL selects an application routing rule to route a Request message and the DSR Application’s Operational Status is “Unavailable”.

**RxApplRuleDuplicatePriority**

- **Measurement Group:** Peer Routing Rules
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Application Routing Rule ID)
- **Description:** Number of times that the application routing rule was selected for routing a message but another application routing rule had the same priority and was ignored.
- **Collection Interval:** 5 min
- **Peg Condition:** When DRL searches the ART and finds more than one highest priority application routing rule with the same priority that matches the search criteria. The measurement is associated with the application routing rule that is selected for routing.

**Recovery:**

- Use GUI screen: Main Menu > Diameter > Configuration > Application Routing Rules to modify peer routing rule priorities.
- At least two application routing rules with the same priority matched an ingress Request message. The system selected the first application routing rule found. Application routing rules must be unique for the same type of messages to avoid unexpected routing results.
RxArtSelected

Measurement Group: Application Routing Rules
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of times that an application routing rule from ART-X was selected for routing a Request message
Collection Interval: 5 min
Peg Condition: When DRL selects an application routing rule from ART-X for routing a message
Measurement Group: Server Group
Recovery:
No action required.

Association Exception measurements

Table 34: Association Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxTrFarEndClose</td>
<td>Number of times the far end closed the SCTP connection.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrManClose</td>
<td>The number of times the Transport was manually closed.</td>
<td>30 min</td>
</tr>
<tr>
<td></td>
<td>This includes manual changes of the transport administrative state that caused the transport to transition from APP-UP to Disabled.</td>
<td></td>
</tr>
<tr>
<td>EvTrNoRespClose</td>
<td>The number of times the Transport was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrCnxFail</td>
<td>The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections. The number of times an open attempt on UDP socket in Listen Mode failed on the Transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxTrSendFail</td>
<td>The number of times the SCTP/UDP sends failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxTrRcvFail</td>
<td>The number of times an SCTP receive attempt failed on the transport. Failure to receive message via SCTP might result in a message being discarded.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrSockInitFail</td>
<td>Number of times the socket initialization failed.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxM3uaERROR</td>
<td>The number of times an M3UA ERROR message is received by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.</td>
<td>30 min</td>
</tr>
<tr>
<td>TmSingleTransQueueFull</td>
<td>The number of egress messages that were discarded because the single Transport Writer Queue was full.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvAsnUpAckTO</td>
<td>Number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during association start-up (when the association is in the Enabled administrative state).</td>
<td>30 min</td>
</tr>
<tr>
<td>RxAsnUnsolDownAck</td>
<td>Number of unsolicited M3UA ASP-DOWN-ACK messages received on the association. Unsolicited ASP-DOWN-ACK messages can be sent by the SG to indicate that the SG cannot process traffic on the association.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxAsnInvalidM3ua</td>
<td>Number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvSctpAdjIPToDwn</td>
<td>Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvSctpTransRej</td>
<td>Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**RxTrFarEndClose**

**Measurement Group:** Association Exception  
**Measurement Type:** Simple  
**Description:** Number of times the far end closed the SCTP connection  
**Collection Interval:** 30 min
**EvTrManClose**

**Measurement Group:** Association Exception

**Measurement Type:** Simple

**Description:** The number of times the association was manually closed. This includes manual changes of the association administrative state that cause the association to transition from ASP-UP to either ASP-DOWN or Disabled.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time a manual change is made to the association administrative state from Enabled to Blocked or from Enabled to Disabled, causing the association to transition out of ASP-UP protocol state.

**Measurement Scope:** NE, Server

**Recovery:**

1. If the association is known to be under maintenance no further action is necessary. If the association was not known to be under maintenance, you can view the Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. View the event history from the GUI main menu under Alarms & Events>View History and look for Event ID 19228. Event ID 19228 shows the manual association state transitions and contains a time-stamp of when the change occurred.
3. View the security logs from the GUI main menu under Security Logs. You can search the logs using the time-stamp from the event history log to determine which login performed the manual state change on the association.
4. Contact My Oracle Support (MOS) for assistance if needed.

**EvTrNoRespClose**

**Measurement Group:** Association Exception

**Measurement Scope:** NE, Server

**Recovery:**

1. If the closing of the association was expected, no further action is necessary, the association will be recovered as soon as the far-end is ready to connect again. If the closing of the association was not expected. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Look in the event history from the GUI main menu under Alarms & Events>View History for Event ID 19224 to determine exactly when the far-end closed the association.
3. Look for other events for the association or MP server in the event history.
4. Verify that IP connectivity still exists between the MP server and the SG.
5. Verify whether the far-end of the association is undergoing maintenance.
6. Contact My Oracle Support (MOS) for assistance if needed.
Measurements

Measurement Type: Simple

Description: The number of times the association was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the association or to SCTP heartbeating if enabled.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an established SCTP association is closed by the MP server due to lack of response at the SCTP level from the far-end of the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. If it has a non-zero value, the association has been closed due to the lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the signaling gateway. You can view the Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Look in the event history from the GUI main menu under Alarms & Events>View History for Event ID 19225.
3. Verify IP connectivity between the MP server and the signaling gateway.
4. Determine if the far-end of the association is congested, possibly causing slow response times on the association.
5. Check the IP network between the MP server and the signaling gateway for excessive retransmissions.
6. Contact My Oracle Support (MOS) for assistance if needed.

EvTrCnxFail

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the SCTP connection attempt failed on the association. This includes only unsuccessful attempts to connect to the signaling gateway. It does not include failure of established connections.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an SCTP connect attempt fails.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the signaling gateway at least once and failed to establish the SCTP connection. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Check the event history log from the GUI main menu under Alarms & Events>View History, looking for Event ID 19222. Event ID 19222 provides details about the cause of the failure.
3. Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address. You can view the Adjacent Servers from the GUI main menu under SS7/Sigtran>Configuration>Adjacent Servers.
4. Verify that the remote port configured for the association correctly identifies the port that the signaling gateway is listening on for SCTP connections. You can view the configured port from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.

5. Verify the IP network connectivity between the MP server and the signaling gateway.

6. If the signaling gateway must be configured to connect to the MP server’s IP address and port, verify that the signaling gateway configuration matches the association configuration. You can view association data from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.

7. Contact *My Oracle Support (MOS)* for assistance if needed.

### TxTrSendFail

**Measurement Group:** Association Exception  
**Measurement Type:** Simple  
**Description:** The number of times the SCTP Send failed for non-DATA M3UA signaling on the association. The number includes the sending of any non-DATA messages on an established association.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an attempt to send M3UA signaling fails for any reason and the information being sent cannot be mapped to a specific link  
**Measurement Scope:** NE, Server  
**Recovery:**

1. This measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this association using SCTP has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association. You can view Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.

2. Look in the GUI main menu under **Alarms & Events>View History** in the event history log for Event ID 19233. **Event ID 19233** provides information on the cause of the failure to send.

3. Verify that the IP network between the MP server and the SG is functioning as expected.

4. Contact *My Oracle Support (MOS)* for assistance if needed.

### RxTrRcvFail

**Measurement Group:** Association Exception  
**Measurement Type:** Simple  
**Description:** The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length.  
**Measurement Scope:** NE, Server
Recovery:

1. This measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.

2. Look in the event history log from the GUI main menu under Alarms & Events>View History for Event ID 19223. Event ID 19223 gives more information about what caused the failure.

3. Try to bring the sockets back into alignment by manually Disabling and Enabling the association.

4. Contact My Oracle Support (MOS) for assistance if needed.

EvTrSockInitFail

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the socket initialization failed. Socket initialization includes configuring the association according to the settings in the GUI under SS7/Sigtran>Configuration>Associations>Configuration Sets.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time one or more socket options cannot be set according to the settings in the association’s configuration set.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value indicates a problem with the association setup prior to attempting to connect the association. If this occurs, look for Event ID 19221 in the GUI under Alarms & Events>View History. Event 19221 provides details about the configuration failure.

2. Contact My Oracle Support (MOS) for further assistance.

RxAsnM3uaERROR

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of M3UA ERROR messages received on the association. An M3UA ERROR message is sent by the far-end to complain about an invalid M3UA message that it received.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA ERROR message is received that cannot be mapped to a specific link.

Measurement Scope: NE, Server

Recovery:

1. This measurement will have a value of zero. A non-zero value indicates a problem with M3UA signaling sent by the MP server.
2. Look for Event ID 19235 from the GUI main menu under Alarms & Events>View History. Event ID 19235 provides more information about the receipt of the ERROR message.

3. If the ERROR reason in Event ID 19235 indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.

4. Contact My Oracle Support (MOS) for assistance if needed.

EvAsnUpAckTO

Measurement Group: Association Exception
Measurement Type: Simple
Description: The number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during the association start-up (when the association is in the Enabled administrative state).
Collection Interval: 30 min
Peg Condition: This measurement is incremented by one each time an ASP-UP has been sent and the M3UA State Management ACK Timer expires, but no ASP-UP-ACK has been received for the association.
Measurement Scope: NE, Server
Recovery:
1. This measurement should have a zero value. If the value is not zero, the association cannot be brought into the state necessary for M3UA ASPTM traffic because the far-end of the association is not responding by sending an ASP-UP-ACK prior to the timeout defined in the GUI under SS7/Sigtran>Configuration>Options>M3UA. The field that defines the timeout is the State Management ACK Timer.
2. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
3. Check the event history from the GUI main menu under Alarms & Events>View History, looking for Event ID 19226. Event ID 19226 will show when the timeout occurred.
4. Verify that the far-end of the association on the SG is not undergoing maintenance.
5. Verify that the State Management ACK Timer value is not set too short. This should not occur if the IP network is functioning correctly.
6. Verify that the IP network between the MP server and the SG is performing up to expectations.
7. Contact My Oracle Support (MOS) for assistance if needed.

RxAsnUnsolDownAck

Measurement Group: Association Exception
Measurement Type: Simple
Description: The number of unsolicited M3UA ASP-DOWN-ACK messages received on the association. Unsolicited ASP-DOWN-ACK messages can be sent by the SG to indicate that the SG cannot process traffic on the association.
Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an unsolicited ASP-DOWN-ACK is received on the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value means that the far-end of the association has stopped processing M3UA signaling. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Check the event history from the GUI main menu under Alarms & Events>View History, looking for Event ID 19227. Event ID 19227 will show exactly when the unsolicited ASP-DOWN-ACK was received.
3. Verify whether the far-end of the association is undergoing maintenance.
4. Contact My Oracle Support (MOS) for assistance if needed.

RxAsnInvalidM3ua

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA message is received on the association that is invalid due to any syntactic or semantic reason.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. In case of a non-zero value in this measurement, review the event history from the GUI main menu under Alarms & Events>View History, looking for Event 19231.
2. Event 19231 provides details about the reason for rejecting the M3UA message. If the error reason indicates a problem with routing context, verify that the routing context used for the association specified in Event 19231 is configured to match between the ASP and the SG.
3. Contact My Oracle Support (MOS) for assistance if needed.

TmSingleTransQueueFull

Measurement Group: Transport Exception

Measurement Type: Simple

Description: The number of egress messages that were discarded because the single Transport Writer Queue was full.

Collection Interval: 30 min
**Peg Condition:** Check whether the single peers transmit data queue limit has reached its max limit (1000). If maximum limit is reached or exceeded, then peg the measurement and discard the low priority events.

**Measurement Scope:** NE, Server

**Recovery:**
This measurement indicates that the Transport is backed up and messages might be discarded. If the value is above the defined critical threshold, an alarm (19408) is generated.

If the problem persists, contact *My Oracle Support (MOS).*

---

**EvSctpAdjPToDwn**

**Measurement Group:** Transport Exception

**Measurement Type:** Simple

**Description:** Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.

**Collection Interval:** 30 min

**Peg Condition:** This measurement shall be incremented by one each time:
- Reachibility to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected.

**Measurement Scope:** NE, Server

**Recovery:**
If all is well, the measurement will have a zero value. A non-zero value indicates that a path fault to that address was detected.

1. Check the event history log at **Main Menu > Alarms & Events > View History**; look for event ID 19410. Event ID 19410 provides more details about the actual cause of the failure.
2. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu > Transport Manager > Configuration > Adjacent Node**.
3. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
4. If the problem persists, contact *My Oracle Support (MOS).*

---

**EvSctpTransRej**

**Measurement Group:** Transport Exception

**Measurement Type:** Simple

**Description:** Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.

**Collection Interval:** 30 min

**Peg Condition:** This measurement shall be incremented by one each time:
The association has been rejected due to IP address validation in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.

**Measurement Scope:** NE, Server

**Recovery:**

If all is well, the measurement has a zero value. A non-zero value indicates that an Adjacent Node has attempted to connect to the Peer IP Address at least once, but the connection attempt was rejected because the IP address advertised by the Adjacent Node failed validation.

1. Check the Transport history at **Main Menu>Transport Manager>Maintenance**.
2. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
3. Verify that the SCTP validation mode is the one that is needed.
4. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu>Transport Manager>Configuration>Adjacent Node**.
5. Verify that the remote port configured at **Main Menu>Transport Manager>Configuration>Transport** for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.
6. If the problem persists, contact **My Oracle Support (MOS)**.

## Association Performance measurements

**Table 35: Association Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxTrOctets</td>
<td>The number of octets sent on the SCTP/UDP Transport. It does</td>
<td>30 min</td>
</tr>
<tr>
<td></td>
<td>not include SCTP, IP, or Ethernet</td>
<td></td>
</tr>
<tr>
<td>RxTrOctets</td>
<td>The number of octets received</td>
<td>30 min</td>
</tr>
<tr>
<td></td>
<td>on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet</td>
<td></td>
</tr>
<tr>
<td>SCTPAssocQueuePeak</td>
<td>The peak SCTP Single Association Writer Queue utilization (0-100%) measured</td>
<td>30 min</td>
</tr>
<tr>
<td></td>
<td>during the collection interval.</td>
<td></td>
</tr>
<tr>
<td>SCTPAssocQueuePeak</td>
<td>The average SCTP Single Association Writer Queue utilization (0-100%)</td>
<td>30 min</td>
</tr>
<tr>
<td></td>
<td>measured during the collection interval.</td>
<td></td>
</tr>
</tbody>
</table>
TxTrOctets

Measurement Group: Transport Performance
Measurement Type: Simple
Description: The number of octets sent on the association. This includes octets for both DATA and non-DATA M3UA signaling. It does not include SCTP, IP, or Ethernet headers.
Collection Interval: 30 min
Peg Condition: This measurement is incremented by the number of octets in the message each time:
  • A DATA/non-DATA message is successfully sent on the transport.
Measurement Scope: NE, Server
Recovery: No action required.

RxTrOctets

Measurement Group: Transport Performance
Measurement Type: Simple
Description: The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.
Collection Interval: 30 min
Peg Condition: This measurement shall be incremented by the number of octets in the message each time:
  • A DATA/non-DATA message is successfully received on the transport.
Measurement Scope: NE, Server
Recovery: No action required.

SCTPAssocQueuePeak

Measurement Group: Association Performance
Measurement Type: Max
Description: The peak SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 30 min
Peg Condition: Transport’s queue is registered as a Stack Resource. The StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.
Measurement Scope: NE, Server
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.
4. Contact My Oracle Support (MOS) for assistance if needed.

**SCTPAssocQueueAvg**

**Measurement Group:** Association Performance  
**Measurement Type:** Average  
**Description:** The average SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 30 min  
**Peg Condition:** The average of all SCTP Single Association Writer Queue utilization samples taken during the collection interval.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. This measurement is a measure of how fast the Transport queue is processed and indicates the Average depth of queue over the monitored interval.  
2. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.  
3. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.  
4. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.  
5. If the problem persists, contact My Oracle Support (MOS).

**Association Usage measurements**

**Table 36: Association Usage Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvTrCnxSuccess</td>
<td>The number of times the SCTP connection was successfully established on the transport. The number of times UDP socket in</td>
<td>30 min</td>
</tr>
</tbody>
</table>
EvTrCnxSuccess

**Measurement Group:** Transport Usage

**Measurement Type:** Simple

**Description:** The number of times the SCTP connection was successfully established on the transport. The number of times the UDP socket in Listen Mode was opened successfully on the Transport.

**Collection Interval:** 30 min

**Peg Condition:** This measurement shall be incremented by one each time:
- The SCTP association reaches the APP-UP protocol state (for example, the connection is successfully established).

  The UDP socket in Listen Mode was opened successfully.

**Measurement Scope:** NE, Server

**Recovery:**

If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise, preform the following steps:

1. You can view the transport status can be viewed from the GUI main menu under **Transport Manager> Maintenance > Transport**.

2. Look in the event history from the GUI main menu under **Alarms & Events > View History**. Look for events related to the association or the MP server to determine what might have caused the association to fail.

3. Contact **My Oracle Support (MOS)** for assistance if needed.
Measurements

TmAsnBlkNotDown

**Measurement Group:** Association Usage

**Measurement Type:** Duration

**Description:** The number of seconds during the reporting interval during which the association was in the Blocked administrative state but was not in ASP-DOWN state. When the association is Blocked, the desired protocol state is ASP-DOWN. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.

**Collection Interval:** 30 min

**Peg Condition:** Time is accumulated for this measurement during the collection interval when all of the following are true:

- The association is in the Blocked administrative state.
- The association is not in the ASP-DOWN protocol state.

**Measurement Scope:** NE, Server

**Recovery:**

1. The value of this measurement should be zero. A non-zero value indicates that the association was set to the Blocked administrative state, but was not able to reach the desired protocol state due to some problem. You can view the Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address. You can check the configuration from the GUI main menu under SS7/Sigtran>Configuration>Adjacent Servers.
3. Verify that the remote port configured for the association correctly identifies the port that the SG is listening on for SCTP connections. You can check the configuration from the GUI main menu under SS7/Sigtran>Configuration>Associations>Configure.
4. Verify the IP network connectivity between the MP server and the SG.
5. If the SG must be configured to connect to the MP server’s IP address and port, verify that the SG configuration matches the association configuration. You can check the configuration from the GUI main menu under SS7/Sigtran>Configuration>Associations>Configure.
6. Contact My Oracle Support (MOS) for assistance if needed.

TmAsnEnaNotUp

**Measurement Group:** Association Usage

**Measurement Type:** Duration

**Description:** The time that the association was enabled, but not in the ASP-UP state

**Collection Interval:** 30 min

**Peg Condition:** Time shall be accumulated for this measurement during the collection interval when all of the following are true:

- the association is in the Enabled administrative state
- the association is not in the ASP-UP protocol state for any reason
Measurement Scope: NE, Server
Recovery:
No action is required.

Charging Proxy Application (CPA) Exception measurements

The CPA Exception measurement group contains measurements that provide information about exceptions and unexpected messages and events that are specific to the CPA application. Measurements in this group include:

- Totals for unexpected/errors associated with message content
- Totals for unexpected/errors associated with message routing

Table 37: CPA Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvCpaMessageDecodeFail</td>
<td>The total number of diameter message decode failures.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaMissingAvp</td>
<td>The total number of diameter messages received without an AVP required for this application.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaOOS</td>
<td>The number of times the CPA was taken Out Of Service.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSubResourceCongested</td>
<td>The total number of Sub-Resources that are determined to be in congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaUnexpectedSess</td>
<td>The CPA has received an ACA-Start that already has a Session Binding Record.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaUnkDiameterAppId</td>
<td>The total number of diameter messages received with an unknown application ID.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaHaSubResourceUnavail</td>
<td>The number of times a Diameter message is received whose Session-Id hashes to a database partition that is unavailable.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaNon2xxAnswer</td>
<td>The number of Diameter Answer messages received with a non-2xx response code.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaOpStatusUnavail</td>
<td>The number of times a message is received and the CPA has an operational status of unavailable.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxCpaUnexpected</td>
<td>The number of Unexpected Diameter message types received during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaAnswerByCpa</td>
<td>The number of times an Answer is generated (not relayed) by the CPA.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaRteFailure</td>
<td>The number of messages sent by the CPA to the routing layer which failed to route successfully.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**EvCpaMessageDecodeFail**

*Measurement Group:* CPA Exception  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* The total number of diameter message decode failures.  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement will be pegged whenever a Diameter message decode failure is detected.  
*Measurement Scope:* Network, NE, Server Group  
*Recovery:*  
  No action required.

**EvCpaMissingAvp**

*Measurement Group:* CPA Exception  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* The total number of diameter messages received without an AVP required for this application.  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement will be pegged whenever a Diameter message is received without an AVP required for this application.  
*Measurement Scope:* Network, NE, Server Group  
*Recovery:*  
  No action required.
EvCpaOOS

Measurement Group: CPA Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of times the CPA was taken Out Of Service.
Collection Interval: 5 min
Peg Condition: This measurement will be incremented when the CPA is taken Out Of Service either manually or automatically.
Measurement Scope: Network, NE, Server Group
Recovery:
1. This measurement indicates problems with the CPA. Logs and Alarms should be checked to determine the cause of the problem.
2. Contact My Oracle Support (MOS) for assistance.

EvCpaSubResourceCongested

Measurement Group: CPA Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Congestion Level)
Description: The total number of Sub-Resources that are determined to be in congestion.
Collection Interval: 5 min
Peg Condition: This measurement will be pegged whenever SBR reports a congestion level either through a response or a polled query.
Measurement Scope: Network, NE, Server Group
Recovery: No action required.

EvCpaUnexpectedSess

Measurement Group: CPA Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The CPA has received an ACA-Start that already has a Session Binding Record.
Collection Interval: 5 min
Peg Condition: This measurement will be incremented when an ACA-Start is received and a Session Binding Record already exists.
**EvCpaUnkDiameterAppId**

**Measurement Group:** CPA Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The total number of diameter messages received with an unknown application ID.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement will be pegged whenever a Diameter message is received with an unknown application ID.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:** No action required.

**RxCpaHaSubResourceUnavail**

**Measurement Group:** CPA Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Sub-Resource ID)  
**Description:** The number of times a Diameter message is received whose Session-Id hashes to a database partition that is unavailable.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement will be incremented when a Diameter request hashes to a database partition that is unavailable.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:** No action required.

**RxCpaNon2xxxAnswer**

**Measurement Group:** CPA Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Diameter Answer messages received with a non-2xxx response code.
**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when an unexpected Diameter answer with a non-2xxx response code is received.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
1. If this count is non-zero it could indicate a mis-configuration of Application Routing.
2. Contact *My Oracle Support (MOS)* for assistance.

### RxCpaOpStatusUnavail

**Measurement Group:** CPA Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of times a message is received and the CPA has an operational status of unavailable.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when a Diameter Request is received when the operational status of the CPA is Unavailable.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**

No action required.

### RxCpaUnexpected

**Measurement Group:** CPA Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of Unexpected Diameter message types received during the reporting interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when an unexpected Diameter (ie; not an Accounting) message is received.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
1. If this count is non-zero it could indicate a mis-configuration of Application Routing.
2. Contact *My Oracle Support (MOS)* for assistance.
Charging Proxy Application (CPA) Performance measurements

The CPA Performance measurement group contains measurements that provide performance information that is specific to the CPA application. Measurements in this group include:

- Totals for various expected/normal messages and events
- Totals for various expected/normal routing procedures invoked
# Table 38: CPA Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxCpaAcaEvent</td>
<td>The number of Accounting Answer-Event messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcaInterim</td>
<td>The number of Accounting Answer-Interim messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcaStart</td>
<td>The number of Accounting Answer-Start messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcaStop</td>
<td>The number of Accounting Answer-Stop messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcrEvent</td>
<td>The number of Accounting Request-Event messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcrInterim</td>
<td>The number of Accounting Request-Interim messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcrStart</td>
<td>The number of Accounting Request-Start messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAcrStop</td>
<td>The number of Accounting Request-Stop messages received during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaMsgProcessed</td>
<td>The total number of Diameter messages (Request or Answer) received during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaAnswerMsgToDrl</td>
<td>The number of Answers sent to DRL layer by CPA during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaMsgCopyInd</td>
<td>The number of messages sent by the CPA to the routing layer</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>with message copy indication set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TxCpaRequestMsgToDrl</td>
<td>The number of Requests sent to DRL layer by CPA during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaTraceInd</td>
<td>The number of messages sent by the CPA to the routing layer with trace indication set.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxCpaAcaEvent**

*Measurement Group:* CPA Performance  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* The number of Accounting Answer-Event messages received during the collection interval.  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement will be incremented when an Accounting Answer-Event message is received by the CPA application.  
*Measurement Scope:* Network, NE, Server Group  
*Recovery:*  
  No action required.

**RxCpaAcaInterim**

*Measurement Group:* CPA Performance  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* The number of Accounting Answer-Interim messages received during the collection interval.  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement will be incremented when an Accounting Answer-Interim message is received by the CPA application.  
*Measurement Scope:* Network, NE, Server Group  
*Recovery:*  
  No action required.
RxCpaAcaStart

**Measurement Group:** CPA Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Accounting Answer-Start messages received during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement will be incremented when an Accounting Answer-Start message is received by the CPA application.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:**  
No action required.

RxCpaAcaStop

**Measurement Group:** CPA Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Accounting Answer-Stop messages received during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement will be incremented when an Accounting Answer-Stop message is received by the CPA application.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:**  
No action required.

RxCpaAccounting

**Measurement Group:** CPA Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Diameter Accounting messages received during the reporting interval.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement will be incremented when a Diameter Accounting message is received.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:**
No action required.

RxCpaAcrEvent

Measurement Group: CPA Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Accounting Request-Event messages received during the collection interval.
Collection Interval: 5 min
Peg Condition: This measurement will be incremented when an Accounting Request-Event message is received by the CPA application.
Measurement Scope: Network, NE, Server Group
Recovery:
   No action required.

RxCpaAcrInterim

Measurement Group: CPA Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Accounting Request-Interim messages received during the collection interval.
Collection Interval: 5 min
Peg Condition: This measurement will be incremented when an Accounting Request-Interim message is received by the CPA application.
Measurement Scope: Network, NE, Server Group
Recovery:
   No action required.

RxCpaAcrStart

Measurement Group: CPA Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Accounting Request-Start messages received during the collection interval.
Collection Interval: 5 min
Measurements

**Peg Condition:** This measurement will be incremented when an Accounting Request-Start message is received by the CPA application.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
No action required.

**RxCpaAcrStop**

**Measurement Group:** CPA Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of Accounting Request-Stop messages received during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when an Accounting Request-Stop message is received by the CPA application.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
No action required.

**RxCpaMsgProcessed**

**Measurement Group:** CPA Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The total number of Diameter messages (Request or Answer) received during the reporting interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be pegged whenever a Diameter message (Request or Answer) is received.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
No action required.

**TxCpaAnswerMsgToDrl**

**Measurement Group:** CPA Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single
Description: The number of Answers sent to DRL layer by CPA during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever CPA sends an Answer to DRL during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery: No action required.

TxCpaMsgCopyInd

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of messages sent by the CPA to the routing layer with message copy indication set.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA sends a message to the routing layer with the message copy indication set.

Measurement Scope: Network, NE, Server Group

Recovery: No action required.

TxCpaRequestMsgToDrl

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Requests sent to DRL layer by CPA during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever CPA sends a Request to DRL during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery: No action required.

TxCpaTraceInd

Measurement Group: CPA Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of messages sent by the CPA to the routing layer with trace indication set.
Collection Interval: 5 min
Peg Condition: This measurement will be incremented when the CPA sends a message to the routing layer with the trace indication set.
Measurement Scope: Network, NE, Server Group
Recovery:
No action required.

Charging Proxy Application (CPA) Session DB measurements

The CPA Session DB measurement group contains measurements that provide information about events that occur when the CPA queries the Session Binding Repository:

• Performance related measurements for SBR queries
• Exceptions and unexpected events related to SBR query processing

Table 39: CPA Session DB Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvCpaNoSbrAccess</td>
<td>The number of queries by the CPA to the SBR where the SBR is inaccessible.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrAvgRespTime</td>
<td>The average response time for a stateful SBR transaction.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrCreateSess</td>
<td>The number of sessions created by the CPA on the SBR during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrDeleteSess</td>
<td>The number of sessions deleted by the CPA on the SBR during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrPeakRespTime</td>
<td>The peak response time for SBR queries during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrQryError</td>
<td>The number of queries initiated by the CPA to the SBR that resulted in an error condition during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrQryMatch</td>
<td>The number of queries initiated by the CPA to the SBR that</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>EvCpaSbrQryNoMatch</td>
<td>The number of queries initiated by the CPA to the SBR that resulted in a no match condition during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrRespTime</td>
<td>This measurement groups responses to SBR queries by the amount of round trip time they took to process. Each bucket will represent the number of responses processed within that time interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvCpaSbrUpdateSess</td>
<td>The number of update session requests sent by the CPA to the SBR during the collection interval. The value does not include created sessions.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaUndeliveredMsg</td>
<td>The total number of messages that ComAgent could not send or for which it did not receive a response.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaSbrQueryTot</td>
<td>The total number of queries (reads / creates / updates / deletes) sent from the CPA to the SBR during the reporting interval.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**EvCpaNoSbrAccess**

**Measurement Group:** CPA Session DB  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of queries by the CPA to the SBR where the SBR is inaccessible.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement will be incremented when the CPA attempts a query when the SBR is inaccessible.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:**  
1. The SBR could be Out Of Service or temporarily down.  
2. Contact *My Oracle Support (MOS)* for assistance.
**EvCpaSbrAvgRespTime**

- **Measurement Group:** CPA Session DB
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** The average response time for a stateful SBR transaction.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is the average response time for SBR transactions.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:** No action required.

**EvCpaSbrCreateSess**

- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of sessions created by the CPA on the SBR during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement will be incremented when the CPA creates a new session based on the session identifier.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:** No action required.

**EvCpaSbrDeleteSess**

- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of sessions deleted by the CPA on the SBR during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement will be pegged whenever CPA deletes a session on the SBR during the collection interval.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:**
Measurements

No action required.

**EvCpaSbrPeakRespTime**
- **Measurement Group:** CPA Session DB
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak response time for SBR queries during the reporting interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement tracks the maximum response time for an SBR query in milliseconds for the reporting interval.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:**
  - No action required.

**EvCpaSbrQryErr**
- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of queries initiated by the CPA to the SBR that resulted in an error condition during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement will be incremented when the CPA initiates a query to the SBR and receives an error response.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:**
  - No action required.

**EvCpaSbrQryMatch**
- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of queries initiated by the CPA to the SBR that resulted in a matching condition during the collection interval.
- **Collection Interval:** 5 min
Measurements

**Peg Condition:** This measurement will be incremented when the CPA initiates a query to the SBR and finds a match based on the session identifier.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**

No action required.

**EvCpaSbrQryNoMatch**

- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of queries initiated by the CPA to the SBR that resulted in a no match condition during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when the CPA initiates a query (read, create, update, delete) to the SBR and finds no match based on the session identifier.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**

No action required.

**EvCpaSbrResponseTime**

- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Response Time Interval)
- **Description:** This measurement groups responses to SBR queries by the amount of round trip time they took to process. Each bucket will represent the number of responses processed within that time interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be pegged for every SBR response received.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**

No action required.

**EvCpaSbrUpdateSess**

- **Measurement Group:** CPA Session DB
- **Measurement Type:** Simple
Measurements

**Measurement Dimension:** Single

**Description:** The number of update session requests sent by the CPA to the SBR during the collection interval. The value does not include created sessions.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when the CPA sends an update request to the SBR.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
No action required.

**RxCpaUndeliveredMsg**

**Measurement Group:** CPA Session DB

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The total number of messages that ComAgent could not send or for which it did not receive a response.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be pegged whenever a ComAgent invokes the Undelivered Message callback.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
No action required.

**TxCpaSbrQueryTot**

**Measurement Group:** CPA Session DB

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The total number of queries (reads / creates / updates / deletes) sent from the CPA to the SBR during the reporting interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is the total number of queries sent by the CPA to the SBR.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
No action required.
### Communication Agent (ComAgent) Exception measurements

The “Communication Agent Exception” measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the Communication Agent protocol.

**Table 40: Communication Agent Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>CADataFIFOQueueFul</td>
<td>StackEvents discarded due to ComAgent DataFIFO queue full condition.</td>
<td>30 min</td>
</tr>
<tr>
<td>CADSTxDscrdCong</td>
<td>Number of egress stack events discarded because the congestion level of the connection exceeded the stack events’ priority level.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSRsrcErr</td>
<td>Number of times that ComAgent receives in a heartbeat stack event status concerning a known Resource but an unknown Sub-Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxDscrdCongSR</td>
<td>Number of stack events discarded due to HA Service Sub-Resource congestion.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxDscrdIntErrSR</td>
<td>Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxDscrdUnavailSR</td>
<td>Number of stack events discarded because they were submitted to an Unavailable Sub-Resource of a given Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxDscrdUnknownSR</td>
<td>Number of egress stack events discarded because they referred to a known Resource and an unknown Sub-Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxDscrdUnkwnRsrc</td>
<td>Number of egress stack events discarded because they referred to an unknown Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxRsrc</td>
<td>Number of egress stack events that were routed to a known Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CAMxFIFOQueueFul</td>
<td>StackEvents discarded due to ComAgent MxFIFO queue full condition.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARsrcPoolFul</td>
<td>ComAgent internal resource pool exhaustion condition</td>
<td></td>
</tr>
<tr>
<td>CARSTxDscrdCong</td>
<td>Number of stack events discarded due to Routed Service congestion.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARSTxDscrdSvcUnavail</td>
<td>Number of stack events discarded because they were submitted to an Unavailable Routed Service.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDiscUnexpEvent</td>
<td>Number of ingress events discarded because it was unexpected in the connection operational state.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdConnUnavail</td>
<td>Number of User Data ingress events discarded because connection was not in-service.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdDecodeFailed</td>
<td>Number of ingress events discarded because failed to deserialize (event not part of stack service language).</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdIncompat</td>
<td>Number of ingress events discarded because an Incompatible header version is received.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdInternalErr</td>
<td>Number of ingress events discarded because of other unexpected internal processing error.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdLayerSendFail</td>
<td>Number of User Data ingress events discarded because layer’s sendTo failed.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdMsgLenErr</td>
<td>Number of ingress events discarded as it doesn’t contain enough bytes (less than event header bytes).</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxDscrdUnkServer</td>
<td>Number of ingress events discarded because the origination server was unknown/not configured.</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CARxDscrdUnkStkLyr</td>
<td>Number of User Data ingress events discarded because stack layer is not known.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxMsgUnknown</td>
<td>Number of ingress events discarded because stack event was unknown.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAStrackQueueFul</td>
<td>StackEvents discarded due to ComAgent task queue full condition.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransDscrdInvCorrId</td>
<td>Number of received stack events that were received and discarded because they did not correlate with a pending transaction.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransDscrdStaleErrRsp</td>
<td>Number of times that an error response was discarded because it contained a valid correlation ID value but its originating server was not the last server to which the request was sent.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAbnorm</td>
<td>Number of reliable transactions that terminated abnormally.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAbnormRateAvg</td>
<td>Average rate per second that ComAgent transactions ended abnormally during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAbnormRateMax</td>
<td>Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAnsErr</td>
<td>Number of reliable transactions initiated by local User Layers that ended with an error response from a destination server.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndErr</td>
<td>Number of reliable transactions initiated by local User Layers that ended abnormally with an error response from a destination server.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndNoResources</td>
<td>Number of reliable transactions initiated by local User Layers that ended abnormally due to lack of resources.</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CATransEndNoResponse</td>
<td>Number of reliable transactions initiated by local User Layers that ended abnormally due to a timeout waiting for a response.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndUnkwnSvc</td>
<td>Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to an unknown service.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndUnregSvc</td>
<td>Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to a known service that lacked a registered User Layer.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransNoReTxMaxTTL</td>
<td>Number of reliable transactions abnormally ended because of Max Time to live exceeded without any retransmits.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransRetx</td>
<td>Number of times stack events were retransmitted.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransReTxExceeded</td>
<td>Number of reliable transactions abnormally ended because of Max number of Retries exceeded.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransStaleSuccessRsp</td>
<td>Number of times that a success response was received from an unexpected server and was accepted to end a transaction.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransTTLExceeded</td>
<td>Number of reliable transactions abnormally ended because of Max Time to live exceeded.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdConnUnAvail</td>
<td>Number of User Data egress events discarded because connection was not in-service(down/blocked/not aligned).</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdDestUserIncompat</td>
<td>Number of User Data egress events discarded because the remote doesn’t support requested capabilities (either it doesn’t support stack or event library or event library version is incompatible)</td>
<td>30 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATxDscrdEncodeFail</td>
<td>Number of User Data egress events discarded because of serialization failures</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdInternalErr</td>
<td>Number of egress events discarded because of other unexpected internal processing error.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdMxSendFail</td>
<td>Number of User Data egress events discarded because of failure reported by MxEndpoint</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdUnknownSvc</td>
<td>Number of non-reliable and non-request (G=0 or R=0) egress stack events discarded because they refer to an unknown service.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdUnkServer</td>
<td>Number of egress events discarded because the destination server was unknown/not configured.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxDscrdUnregSvc</td>
<td>Number of egress stack events discarded because they reference a known service that has no registered User Layer.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**CADataFIFOQueueFul**

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** StackEvents discarded due to ComAgent DataFIFO queue full condition. This value provides a measure of how many messages are discarded by ComAgent due to ComAgent User Data FIFO Queue full condition.  
**Collection Interval:** 30 min  
**Peg Condition:** For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent User Data FIFO queue.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.
If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. Contact My Oracle Support (MOS) for assistance.

CADSTxDscrdCong

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of egress stack events discarded because the congestion level of the connection exceeded the stack events’ priority level.
Collection Interval: 30 min
Peg Condition: When ComAgent receives a stack event from a local User Layer to be transferred via the direct service and the selected connection has a congestion level greater than the priority level of the stack event.
Measurement Scope: Server
Recovery:
When this measurement is increasing, it is an indication that the product is experiencing overload.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine if the offered load is expected and exceeds the product’s capacity.

   If the load is expected and exceeds the product’s capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.

2. Contact My Oracle Support (MOS) for assistance.

CAHSTxDscrdIntErrSR

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Resource ID)
Description: Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.
Collection Interval: 30 min
Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Sub-Resource and that is discarded due to a ComAgent internal error
Measurement Scope: Server
Recovery:

1. Check other ComAgent measurements, alarms, and events to determine the source of the abnormality causing this measurement to arise.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**CAHSTxDscrdfCongSR**

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Resource ID)  
**Description:** Number of stack events discarded due to HA Service Sub-Resource congestion. During normal operation, this measurement should not be increasing. When this measurement is increasing, it is an indication that the product is experiencing overload.  
**Collection Interval:** 30 min  
**Peg Condition:** Stack event submitted to ComAgent by a local User Layer, and the stack event references an HA Service Sub-Resource that has a congestion level greater than the priority level of the stack event.  
**Measurement Scope:** Server  
**Recovery:**  
1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine if the offered load is expected and exceeds the product’s capacity.  
   If the load is expected and exceeds the product’s capacity, then the capacity should be increased so that the overload condition does not persist or reoccur. If the load does not exceed the product’s capacity, then check the status of the servers hosting the Resource Providers to trouble-shoot the cause of the overload.  
   This measurement may not indicate an error if the discarded stack event was a reliable request, the Reliable Transfer Function was able to re-attempt, and the subsequent attempt got through.
2. Contact *My Oracle Support (MOS)* for assistance.

**CAHSTxDscrdfIntErrSR**

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Resource ID)  
**Description:** Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.  
**Collection Interval:** 30 min  
**Peg Condition:** User Layer submits to ComAgent an egress stack event destined to a known Sub-Resource and that is discarded due to a ComAgent internal error.
### CAHSTxDscrdUnavailSR

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Resource ID)  
**Description:** Number of stack events discarded because they were submitted to an Unavailable Sub-Resource of a given Resource. During normal operation, this measurement should not be increasing. Each count of this measurement indicates that a local application attempted to send a stack event to another server using an HA Service Sub-Resource, but the event was discarded due to the Sub-Resource being unavailable.  
**Collection Interval:** 30 min  
**Peg Condition:** Stack event submitted to ComAgent by a local User Layer, and the stack event references an Unavailable Sub-Resource.  
**Measurement Scope:** Server  
**Recovery:**  
1. Use **Main Menu > Comamunication Agent > Maintenance > HA Services Status** to diagnose the cause of routing failures.  
   If a discarded stack event was a request from a reliable transaction and the routing failure was due to a temporary condition, then it is possible that the transaction completed successfully using one or more retransmit attempts.  
   This measurement may not indicate an error if the discarded stack event was a reliable request, the Reliable Transfer Function was able to re-attempt, and the subsequent attempt got through.  
2. Contact **My Oracle Support (MOS)** for assistance.

### CAHSTxDscrdUnknownSR

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Resource ID)  
**Description:** Number of egress stack events discarded because they referred to a known Resource and an unknown Sub-Resource. During normal operation this measurement should be 0. A non-zero value for this measurement indicates that ComAgent is improperly configured to support a local application.  
**Collection Interval:** 30 min
Peg Condition: User Layer submits to ComAgent an egress stack event that refers to an unknown Sub-Resource.

Measurement Scope: Server

Recovery:

1. Use Main Menu > Comamunication Agent > Maintenance > HA Services Status to verify that all HA Service Sub-Resources expected by local applications are present and operating.
2. Contact My Oracle Support (MOS) for assistance.

CAHSTxDscrdUnkwnRsrc

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of egress stack events discarded because they referred to an unknown Resource.
Collection Interval: 30 min
Peg Condition: User Layer submits to ComAgent an egress stack event that refers to an unknown Resource.
Measurement Scope: Server

Recovery:

1. Use Main Menu > Comamunication Agent > Maintenance > HA Services Status to verify that all HA Service Sub-Resources expected by local applications are present and operating.
2. Contact My Oracle Support (MOS) for assistance.

CAHSTxRsnc

Measurement Group: ComAgent Performance, ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Resource ID)
Description: Number of egress stack events that were routed to a known Resource.
Collection Interval: 30 min
Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Resource.
Measurement Scope: Server

Recovery:

No action required.

CAMxFIFOQueueFul

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single

Description: StackEvents discarded due to ComAgent MxFIFO queue full condition. This value provides a measure of how many messages are discarded by ComAgent due to ComAgent internal connection MxFIFO Queue full condition.

Collection Interval: 30 min

Peg Condition: For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent internal connection MxFIFO queue.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. Contact My Oracle Support (MOS) for assistance.

CARsrcPoolFul

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single

Description: ComAgent internal resource pool exhaustion condition.

Collection Interval: 30 min

Peg Condition: This is to track the measure of the internal resource (Ex: CommMessage Resource pool) exhaustion condition for a given interval.

For each resource allocation/access attempt that result in resource pool manager returning an indication that the maximum resources reserved are allocated and are in-use. When this condition occurs ComAgent tries to allocate a new resource from heap and relists it after its life cycle (Ex: CommMessage objects required for user data traffic for MxEndpoint interface).

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many times pre-allocated resources are exhausted in ComAgent interfaces.

This measurement is primarily intended for performance analysis and to assist in evaluating the need for any additional engineering processing capacity or tuning.
CARSTxDscrdCong

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Number of stack events discarded due to Routed Service congestion.  
**Collection Interval:** 30 min  
**Peg Condition:** Stack event submitted to ComAgent by a local User Layer, and the stack event references a Routed Service that has a congestion level greater than the priority level of the stack event.  
**Measurement Scope:** Server  
**Recovery:**  
1. Check the **Main Menu > Communication Agent > Maintenance > Routed Services Status** and **Main Menu > Communication Agent > Maintenance > Connection Status** screens to determine if the offered load is expected and exceeds the product’s capacity.  
   If the load is expected and exceeds the product’s capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.  
2. Contact **My Oracle Support (MOS)** for assistance.

CARSTxDscrdInternalErr

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Number of egress events discarded because of another Routed Service internal error  
**Collection Interval:** 30 min  
**Peg Condition:** Each time an egress event is discarded because of another Routed Service internal error  
**Measurement Scope:** Server  
**Recovery:**  
   Contact **My Oracle Support (MOS)** for assistance.

CARSTxDscrdSvcUnavail

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Number of stack events discarded because they were submitted to an Unavailable Routed Service.
Collection Interval: 30 min

Peg Condition: Stack event submitted to ComAgent by a local User Layer, and the stack event references an Unavailable Routed Service.

Measurement Scope: Server

Recovery:
Each count of this measurement indicates that a local application attempted to send a stack event to another server using a Routed Service, but the event was discarded due to the Routed Service being unavailable. Routing failures can occur due to:

• Maintenance actions are performed that result in a loss of communication between servers.
• Network problems result in a loss of communication between servers.
• Server overload can result in routes becoming unavailable for some stack events.

1. Check the Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status screens to further diagnose the cause of routing failures.

If a discarded stack event was a request from a reliable transaction and the routing failure was due to a temporary condition, then it is possible that the transaction completed successfully using one or more retransmit attempts.

2. Contact My Oracle Support (MOS) for assistance.

CARxDiscUnexpEvent

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single

Description: Number of ingress events discarded because it was unexpected in the connection operational state.

Collection Interval: 30 min

Peg Condition: For each ingress StackEvent that is discarded by ComAgent Stack, due to StackEvent received in unexpected connection state.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to message received in unexpected connection state.

CARTxDscrdBundle

Measurement Group: ComAgent Exception
Measurement Dimension: Single
Measurements

Measurement Type: Simple
Description: Number of ingress bundled event discarded during routing.
Peg Condition: Each time an ingress bundled event is discarded during routing
Collection Interval: 30 min
Measurement Scope: Site
Recovery: No action required

CARxDscrDConnUnavail
Measurement Group: ComAgent Exception
Measurement Type: Simple
Description: Number of User Data ingress events discarded because connection was not in-service.
Collection Interval: 30 min
Peg Condition: For each User Data ingress StackEvent received from configured service peer server with connection status not “in-service”.
Measurement Scope: NE, Server
Recovery: No action required.
This value provides a measure of how many User Data ingress messages are discarded by ComAgent for the data messages received in connection not in “in-service” state.

CARxDscrDDecodeFailed
Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of ingress events discarded because failed to deserialize (event not part of stack service language).
Collection Interval: 30 min
Peg Condition: For each StackEvent received from a configured peer server that resulted in any decode failures within ComAgent Stack.
Measurement Scope: NE, Server
Recovery: No action required.
This value provides a measure of how many ingress messages are discarded by ComAgent due to internal decode error condition.
CARxDscrdIncompat

**Measurement Group:** ComAgent Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of ingress events discarded because an Incompatible header version is received.

**Collection Interval:** 30 min

**Peg Condition:** For each ingress StackEvent that is discarded by ComAgent Stack, due to unsupported base header version, as indicated in StackEvent.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to incompatible base header version of base software event library.

CARxDscrdInternalErr

**Measurement Group:** ComAgent Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of ingress events discarded because of other unexpected internal processing error.

**Collection Interval:** 30 min

**Peg Condition:** For each ingress StackEvent that is discarded by ComAgent Stack, due to internal processing errors for conditions not covered by other meas-pegs.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to internal software processing errors for conditions not covered by other measurement pegs.

CARxDscrdLayerSendFail

**Measurement Group:** ComAgent Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of User Data ingress events discarded because layer’s sendTo failed.
Collection Interval: 30 min

**Peg Condition:** For each User Data StackEvent received from a configured service peer server and resulted in send failure to the destination stack layer.

**Measurement Scope:** NE, Server

**Recovery:**

- No action required.

This value provides a measure of how many User Data ingress messages are discarded by ComAgent due to internal send failure to destination stack layer.

### CARxDscrdMsgLenErr

- **Measurement Group:** ComAgent Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of ingress events discarded as it doesn’t contain enough bytes (less than event header bytes).

**Collection Interval:** 30 min

**Peg Condition:** For each StackEvent received from configured peer with message size less than the minimum required Header.

**Measurement Scope:** NE, Server

**Recovery:**

- No action required.

This value provides a measure of how many ingress messages are discarded by Communication Agent due to message size error.

### CARxDscrdUnkServer

- **Measurement Group:** ComAgent Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of ingress events discarded because the origination server was unknown/not configured.

**Collection Interval:** 30 min

**Peg Condition:** For each ingress StackEvent that is discarded by ComAgent Stack, due to unknown origination ip address contents in StackEvent.

**Measurement Scope:** NE, Server

**Recovery:**
No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to unknown origination ip address in StackEvent.

**CARxDscrdUnkStkLyr**
- **Measurement Group:** ComAgent Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of User Data ingress events discarded because stack layer is not known.
- **Collection Interval:** 30 min
- **Peg Condition:** For each User Data ingress StackEvent received by Communication Agent Stack, for an unknown destination stack.
- **Measurement Scope:** NE, Server

**Recovery:**
- No action required.
- This value provides a measure of how many ingress messages are discarded by Communication Agent, as the destination stack is not registered/known.

**CARxMsgUnknown**
- **Measurement Group:** ComAgent Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of ingress events discarded because stack event was unknown.
- **Collection Interval:** 30 min
- **Peg Condition:** For each undefined StackEvent received from one of the configured peer server.
- **Measurement Scope:** NE, Server

**Recovery:**
- No action required.
- This value provides a measure of how many ingress messages are discarded by ComAgent as the message is not defined/known to ComAgent Stack.

**CAStackQueueFul**
- **Measurement Group:** ComAgent Exception
- **Measurement Type:** Simple
Measurement Dimension: Arrayed

Description: StackEvents discarded due to ComAgent task queue full condition.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent Egress Task Queue.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

3. Contact My Oracle Support (MOS) for assistance.

CATransDscrdInvCorrId

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of received stack events that were received and discarded because they did not correlate with a pending transaction.

Collection Interval: 30 min

Peg Condition: ComAgent receives a response stack event that contains a correlation ID that does not match a pending transaction record.

Measurement Scope: Server

Recovery:

This measurement indicates that one or more destination servers are either responding to requests after a transaction has ended or are sending invalid responses. Contact My Oracle Support (MOS) for assistance.

CATransDscrdStaleErrRsp

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of times that an error response was discarded because it contained a valid correlation ID value but its originating server was not the last server to which the request was sent.

Collection Interval: 30 min
**Peg Condition:** ComAgent receives an error response stack event that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent.

**Measurement Scope:** Server

**Recovery:**

This measurement indicates that one or more servers are responding with errors to requests after the local ComAgent has retransmitted the requests to other destination servers. This could occur due to:

- Network problems result in intermittent loss of communication between servers.
- Server overload results in delayed responses

1. **Use** [Main Menu > Communication Agent > Maintenance > Routed Services Status](#) and [Main Menu > Communication Agent > Maintenance > Connection Status](#) to check the status of the far-end servers and look for signs of overload.
2. **Contact** My Oracle Support (MOS) for assistance.

**CATransEndAbnorm**

**Measurement Group:** ComAgent Exception, ComAgent Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Service ID)

**Description:** Number of reliable transactions that terminated abnormally.

**Collection Interval:** 30 min

**Peg Condition:**

- Transaction times-out waiting for a response, and the maximum number of transmits has been reached.
- Transaction time-to-live limit is exceeded.
- Transaction terminated due to lack of resources.

**Note:** This measurement is NOT pegged for these conditions:

- Transaction involves an unknown service.
- Transaction involves an unregistered Routed Service.

**Measurement Scope:** Server

**Recovery:**

1. Check the ComAgent Exception report to further diagnose the reasons why transactions are failing.
2. Contact My Oracle Support (MOS) for assistance.

**CATransEndAbnormRateAvg**

**Measurement Group:** ComAgent Performance

**Measurement Type:** Average

**Measurement Dimension:** Arrayed (by Service ID)
**Description**: Average rate per second that ComAgent transactions ended abnormally during the collection interval.

**Collection Interval**: 30 min

**Peg Condition**: Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.

**Measurement Scope**: Server

**Recovery**:
This measurement provides the average rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

**CATransEndAbnormRateMax**

**Measurement Group**: ComAgent Performance

**Measurement Type**: Max

**Measurement Dimension**: Arrayed (by Service ID)

**Description**: Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.

**Collection Interval**: 30 min

**Peg Condition**: Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.

**Measurement Scope**: Server

**Recovery**:
This measurement provides the maximum rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

**CATransEndAnsErr**

**Measurement Group**: ComAgent Exception

**Measurement Type**: Simple

**Measurement Dimension**: Arrayed (by Service ID)

**Description**: Number of reliable transactions initiated by local User Layers that ended with an error response from a destination server.

**Collection Interval**: 30 min

**Peg Condition**: When a reliable response stack event (G=1, A=1, E=1) is received from a server to which a request was sent, and the response corresponds to a pending transaction record.
Measurement Scope: Server

Recovery:

No action necessary.

This measurement has value when compared against other measurements. Server applications may respond with errors as part of normal operations, as seen by ComAgent.

**CATransEndErr**

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Number of reliable transactions initiated by local User Layers that ended abnormally with an error response from a destination server.  
**Collection Interval:** 30 min  
**Peg Condition:** When a valid reliable response stack event (G=1, A=0, E=1) is received from a server to which a request was sent, and the response corresponds to a pending transaction record.

Recovery:

This measurement indicates that one or more destination servers are unable to process reliable requests received from the local server. This can be caused due to maintenance actions, server overload, and unexpected conditions in software.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.  
2. Contact My Oracle Support (MOS) for assistance.

**CATransEndNoResources**

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Number of reliable transactions initiated by local User Layers that ended abnormally due to lack of resources.  
**Collection Interval:** 30 min  
**Peg Condition:** ComAgent receives a reliable request (G=1, R=1) from a local User Layer and ComAgent is unable to allocate resources to process the transaction.

Recovery:
This measurement indicates that the local server is exhausting its resources for processing reliable transactions. This can result when the combination of transaction rate and response delays exceeds engineered limits. High transaction rates can result from local server overload. Excess response delays can result from overloaded destination servers and problems in the network between servers.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.

2. Contact My Oracle Support (MOS) for assistance.

CATransEndNoResponse

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of reliable transactions initiated by local User Layers that ended abnormally due to a timeout waiting for a response.
Collection Interval: 30 min
Peg Condition: Limit on the number of retransmits is reached with no response and limit on the transaction time-to-live is exceeded.
Measurement Scope: Server

Recovery:

This measurement indicates that one or more destination servers are unable to process reliable requests received from the local server. This can be caused due to maintenance actions, server overload, and unexpected conditions in software.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.

2. Contact My Oracle Support (MOS) for assistance.

CATransEndUnkwnSvc

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to an unknown service.
Collection Interval: 30 min
Peg Condition: ComAgent receives a reliable request (G=1, R=1) from a local User Layer that refers to an unknown service.
Measurement Scope: Server
Recovery:
This measurement indicates improper configuration of ComAgent and/or a User Layer application.

1. Use Main Menu > Communication Agent > Configuration > Routed Services to confirm that all services expected by local applications are present.
2. Contact My Oracle Support (MOS) for assistance.

CATransEndUnregSvc

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to a known service that lacked a registered User Layer.
Collection Interval: 30 min
Peg Condition: ComAgent receives a reliable request (G=1, R=1) from a local User Layer that refers to a known service that has no registered User Layer.
Measurement Scope: Server
Recovery:
A non-zero value in this measurement indicates a software malfunction.
Contact My Oracle Support (MOS) for assistance.

CATransNoReTxMaxTTL

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of reliable transactions abnormally ended because of Max Time to live exceeded without any retransmits.
Collection Interval: 30 min
Peg Condition: Maximum Time To Live period exceeded with no retransmission attempts and no response received for the transaction.
Measurement Scope: Server
Recovery:
This measurement provides a measure of abnormal transactions due to maximum time to live period exceeded condition (Without any retransmits) and no response is received from remote. Such abnormal transactions can be due to:
- Server overload that can result in delayed responses.
- Unexpected conditions in software.
Measurements

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.
2. Contact My Oracle Support (MOS) if assistance is needed

CATransRetx

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of times stack events were retransmitted.
Collection Interval: 30 min
Peg Condition: ComAgent reliable transaction retransmit timer expires and the limit on the number of retransmits has not been reached.
Measurement Scope: Server
Recovery:
When this measurement is increasing, it indicates that communication between servers is experiencing unexpectedly high latency and/or packet loss. Retransmissions can occur due to:

- Maintenance actions are performed that result in a loss of communication between servers.
- Network problems result in a loss of communication between servers.
- Server overload can result in delayed responses.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.
2. Contact My Oracle Support (MOS) for assistance.

CATransReTxExceeded

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of reliable transactions abnormally ended because of Max number of Retries exceeded.
Collection Interval: 30 min
Peg Condition: Number of retransmits limit is reached with no response received for the transaction.
Measurement Scope: Server
Recovery:
This measurement provides a measure of abnormal transactions due to maximum number of retransmission exceeded condition awaiting response from remote. Such abnormal transactions can be due to:
• Maintenance actions performed that result in a loss of communication between servers.
• Server overload that can result in delayed responses.
• Unexpected conditions in software.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.
2. Contact My Oracle Support (MOS) if assistance is needed

CATransStaleSuccessRsp

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of times that a success response was received from an unexpected server and was accepted to end a transaction.
Collection Interval: 30 min
Peg Condition: ComAgent receives a success response stack event (G=1, A=1, E=1) that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent.
Measurement Scope: Server
Recovery:

This measurement indicates that a Routed Service received a success response from an unexpected server. This most commonly occurs if a server is slow to respond, ComAgent retransmits a request to another server, and then the original server finally responds to the request.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to diagnose stale responses.
2. Contact My Oracle Support (MOS) for assistance.

CATransTTLExceeded

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of reliable transactions abnormally ended because of Max Time to live exceeded.
Collection Interval: 30 min
Peg Condition: Maximum Time To Live period exceeded with at least one retransmission attempted and no response received for the transaction.
Measurement Scope: Server
Recovery:
This measurement provides a measure of abnormal transactions due to maximum time to live period exceeded condition (Where at least one retransmission was also attempted) and no response is received from remote. Such abnormal transactions can be due to:

- Maintenance actions performed that result in a loss of communication between servers.
- Server overload that can result in delayed responses.
- Unexpected conditions in software.

1. Use Main Menu > Communication Agent > Maintenance > Routed Services Status and Main Menu > Communication Agent > Maintenance > Connection Status to determine network and server communications.

2. Contact My Oracle Support (MOS) if assistance is needed

### CATxDscrdBundle

**Measurement Group:** ComAgent Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** Number of egress bundled event discarded during routing.  
**Peg Condition:** Each time an egress bundled event is discarded during routing  
**Collection Interval:** 30 min  
**Measurement Scope:** Site  
**Recovery:**  
- No action required

### CATxDscrdConnUnAvail

**Measurement Group:** ComAgent Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of User Data egress events discarded because connection was not in-service(down/blocked/not aligned).  
**Collection Interval:** 30 min  
**Peg Condition:** For each User Data egress StackEvent that is discarded by ComAgent Stack, due to connection status not being in-service.  
**Measurement Scope:** NE, Server  
**Recovery:**  
- No action required.

This value provides a measure of how many User Data egress messages are discarded by ComAgent due to connection unavailability reasons.
CATxDscrdDestUserIncmpat

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of User Data egress events discarded because the remote doesn’t support requested capabilities (either it doesn’t support stack or event library or event library version is incompatible).
Collection Interval: 30 min
Peg Condition: For each User Data egress StackEvent that is discarded by Communication Agent Stack, due to incompatibility in requested library id/version and the one known by Communication Agent.
Measurement Scope: NE, Server
Recovery: No action required.
This value provides a measure of how many User Data egress messages are discarded by Communication Agent due to remote not supporting requested capabilities.

CATxDscrdEncodeFail

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of User Data egress events discarded because of serialization failures.
Collection Interval: 30 min
Peg Condition: For each User Data egress StackEvent that is discarded by Communication Agent Stack, due to any local encode failures.
Measurement Scope: NE, Server
Recovery: No action required.
This value provides a measure of how many User Data egress messages are discarded by Communication Agent due to local encode failure.

CATxDscrdInternalErr

Measurement Group: ComAgent Exception
Measurement Type: Simple
Measurement Dimension: Single
**Measurements**

**Description:** Number of egress events discarded because of other unexpected internal processing error.

**Collection Interval:** 30 min

**Peg Condition:** For each egress StackEvent that is discarded by ComAgent Stack, due to internal processing errors for conditions not covered by other meas-pegs.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of how many egress messages are discarded by ComAgent due to internal software processing errors for conditions not covered by other measurement pegs.

**CATxDscrdMxSendFail**

**Measurement Group:** ComAgent Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of User Data egress events discarded because of failure reported by MxEndpoint.

**Collection Interval:** 30 min

**Peg Condition:** For each User Data egress StackEvent that is discarded by Communication Agent Stack, due to send failure as indicated by underlying transport.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of how many User Data egress messages are discarded by Communication Agent due to transport reported error condition.

**CATxDscrdUnknownSvc**

**Measurement Group:** ComAgent Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of non-reliable and non-request (G=0 or R=0) egress stack events discarded because they refer to an unknown service. This measurement indicates that ComAgent is improperly configured to support a local application.

**Collection Interval:** 30 min

**Peg Condition:** User Layer submits to ComAgent a non-reliable or non-request (G=0 or R=0) egress stack event that refers to an unknown service.

**Measurement Scope:** Server
Recovery:
1. Use Main Menu > Communication Agent > Configuration > Routed Services screen to verify that all Routed Services expected by local applications are properly configured.
2. Contact My Oracle Support (MOS) for assistance.

CATxDscrdUnkServer
- Measurement Group: ComAgent Exception
- Measurement Type: Simple
- Measurement Dimension: Single
- Description: Number of egress events discarded because the destination server was unknown/not configured.
- Collection Interval: 30 min
- Peg Condition: For each egress StackEvent that is discarded by ComAgent Stack, due to unknown destination ip address contents in StackEvent.
- Measurement Scope: NE, Server
- Recovery:
  - No action required.
  - This value provides a measure of how many egress messages are discarded by ComAgent due to unknown destination ip address in StackEvent.

CATxDscrdUnregSvc
- Measurement Group: ComAgent Exception
- Measurement Type: Simple
- Measurement Dimension: Arrayed (by Service ID)
- Description: Number of egress stack events discarded because they reference a known service that has no registered User Layer.
- Collection Interval: 30 min
- Peg Condition: User Layer submits to ComAgent an egress stack event that refers to a known service that lacks a registered User Layer.
- Measurement Scope: Server
- Recovery:
  - A non-zero measurement indicates that a local application is malfunctioning and is attempting to use a service for which it has not registered. Contact My Oracle Support (MOS) for assistance.
Communication Agent (ComAgent) Performance measurements

The "Communication Agent Performance" measurement group is a set of measurements that provide performance information that is specific to the Communication Agent protocol. These measurements will allow the user to determine how many messages are successfully forwarded and received to and from each DSR Application.

Table 41: Communication Agent Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAAvgDataFIFOQueueUtil</td>
<td>Average percentage of ComAgent DataFIFO Queue Utilization</td>
<td>30 min</td>
</tr>
<tr>
<td>CAAvgMxFIFOQueueUtil</td>
<td>Average percentage of ComAgent MxFIFO Queue Utilization</td>
<td>30 min</td>
</tr>
<tr>
<td>CAAvgQueueUtil</td>
<td>Average percentage of Queue Utilization.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAAvgRsrcPoolUtil</td>
<td>Average percentage of internal resource pool utilization</td>
<td>30 min</td>
</tr>
<tr>
<td>CAAvgRxStackEvents</td>
<td>Average Number of User Data ingress events received.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAAvgTxStackEvents</td>
<td>Average Number of User Data egress events received from stacks to deliver it to remote.</td>
<td>30 min</td>
</tr>
<tr>
<td>CADSTx</td>
<td>Number of User Data egress events specifically for the default Direct Service.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxRsrc</td>
<td>Number of egress stack events that were routed to a known Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxRsrcRateAvg</td>
<td>Average rate per second of egress stack events routed to a known Resource.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAHSTxRsrcRateMax</td>
<td>Maximum rate per second of egress stack events routed to a known Resource</td>
<td>30 min</td>
</tr>
<tr>
<td>CAPeakDataFIFOQueueUtil</td>
<td>Maximum percentage of ComAgent DataFIFO Queue Utilization</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CAPeakMxFIFOQueueUtil</td>
<td>Maximum percentage of ComAgent MxFIFO Queue Utilization.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAPeakQueueUtil</td>
<td>Maximum percentage of Queue Utilization.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAPeakRsrcPoolUtil</td>
<td>Maximum percentage of internal resource pool utilization.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAPeakRxStackEvents</td>
<td>Maximum Number of User Data ingress events received.</td>
<td>30 min</td>
</tr>
<tr>
<td>CAPeakTxStackEvents</td>
<td>Maximum Number of User Data egress events received from stacks to deliver it to remote.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARSTx</td>
<td>Number of stack events submitted to a Routed Service for routing.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARx</td>
<td>Number of User Data ingress events received from a peer server.</td>
<td>30 min</td>
</tr>
<tr>
<td>CARxSuccess</td>
<td>Number of User Data ingress events successfully routed to local layers.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAbnorm</td>
<td>Number of reliable transactions that terminated abnormally.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAbnormRateAvg</td>
<td>Average rate per second that ComAgent transactions ended abnormally during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndAbnormRateMax</td>
<td>Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransEndNorm</td>
<td>Number of reliable transactions initiated by local User Layers that ended normally with a response from a destination server.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransPendingAvg</td>
<td>Average number of allocated pending transaction records over the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransPendingMax</td>
<td>Maximum number of allocated pending transaction records.</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>CATransRateAvg</td>
<td>Average rate per second that ComAgent transactions were started during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransRateMax</td>
<td>Maximum rate per second that ComAgent transactions were started during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransStarted</td>
<td>Number of reliable transactions initiated by local User Layers.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransTimeAvg</td>
<td>Average transaction life-time in milliseconds.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATransTimeMax</td>
<td>Maximum transaction life-time in milliseconds.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATx</td>
<td>Number of User Data egress events received on Communication Agent task queue from local stacks to deliver it to a peer server.</td>
<td>30 min</td>
</tr>
<tr>
<td>CATxSuccess</td>
<td>Number of User Data egress events successfully delivered to a peer server.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**CAAvgDataFIFOQueueUtil**

**Measurement Group:** ComAgent Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed  
**Description:** Average percentage of ComAgent DataFIFO Queue Utilization.  
**Collection Interval:** 30 min  
**Peg Condition:** The average ComAgent connection DataFIFO Queue utilization sample taken during the collection interval.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. This measurement is primarily intended to assist in evaluating any issues with ComAgent User Data StackEvent processing and thread scheduling.  

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.
If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. Contact My Oracle Support (MOS) for assistance.

CAAvgMxFIFOQueueUtil

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Arrayed
- **Description:** Average percentage of ComAgent MxFIFO Queue Utilization.
- **Collection Interval:** 30 min
- **Peg Condition:** The average ComAgent connection MxFIFO Queue utilization sample taken during the collection interval.
- **Measurement Scope:** NE, Server

**Recovery:**

1. This measurement is primarily intended to assist in evaluating any issues with internal StackEvent processing and thread scheduling.
   
   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.
   
   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. Contact My Oracle Support (MOS) for assistance.

CAAvgQueueUtil

- **Measurement Group:** ComAgent Exception
- **Measurement Type:** Average
- **Measurement Dimension:** Arrayed
- **Description:** Average percentage of Queue Utilization.
- **Collection Interval:** 30 min
- **Peg Condition:** The average ComAgent Egress Task Queue utilization sample taken during the collection interval.
- **Measurement Scope:** NE, Server

**Recovery:**

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. Contact My Oracle Support (MOS) for assistance.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact *My Oracle Support (MOS)* for assistance.

**CAAvgRsrcPoolUtil**

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Average percentage of internal resource pool utilization.
- **Collection Interval:** 30 min
- **Peg Condition:** This is to track the measure of average usage of the internal resource (Ex: CommMessage Resource pool) for a given interval.
- **Measurement Scope:** NE, Server

**Recovery:**

This measurement is primarily intended to assist in evaluating the need for additional processing or performance capacity tuning on a node.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of a node over several collection intervals, then the internal engineering resource pool capacity or other dependent parameters may need to be tuned, so that it does not result in unaccounted latency.

**CAAvgRxStackEvents**

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Average Number of User Data ingress events received.
- **Collection Interval:** 30 min
- **Peg Condition:** The average User Data ingress StackEvent sample taken during the collection interval.
- **Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of Average Value during the interval, for number of User Data messages received from remote.
**CAAvgTxStackEvents**

- **Measurement Group**: ComAgent Performance
- **Measurement Type**: Average
- **Measurement Dimension**: Single
- **Description**: Average Number of User Data egress events received from stacks to deliver it to remote.
- **Collection Interval**: 30 min
- **Peg Condition**: The average User Data egress StackEvent sample taken during the collection interval.
- **Measurement Scope**: NE, Server
- **Recovery**: No action required.
  
  This value provides a measure of Average Value during the interval, for number of User Data messages transmitted to remote.

**CADSTx**

- **Measurement Group**: ComAgent Performance
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: Number of User Data egress events specifically for the default Direct Service.
- **Collection Interval**: 30 min
- **Peg Condition**: For each User Data egress StackEvent received specifically for the default Direct Service and processed by ComAgent Stack.
- **Measurement Scope**: NE, Server
- **Recovery**: No action required.
  
  This value provides a measure of how many User Data egress messages are received by ComAgent to be transmitted from hosting server to destined remote server using default Direct “EventTransfer” Service.

**CAHSTxRsrc**

- **Measurement Group**: ComAgent Performance, ComAgent Exception
- **Measurement Type**: Simple
- **Measurement Dimension**: Arrayed (by Resource ID)
- **Description**: Number of egress stack events that were routed to a known Resource.
- **Collection Interval**: 30 min
Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Resource.
Measurement Scope: Server
Recovery: No action required.

CAHSTxRsrcRateAvg
Measurement Group: ComAgent Performance
Measurement Type: Average
Measurement Dimension: Arrayed (by Resource ID)
Description: Average rate per second of egress stack events routed to a known Resource.
Collection Interval: 30 min
Peg Condition: Based upon the SysMetric.
Measurement Scope: Server
Recovery: No action required.

CAHSTxRsrcRateMax
Measurement Group: ComAgent Performance
Measurement Type: Max
Measurement Dimension: Arrayed (by Resource ID)
Description: Maximum rate per second of egress stack events routed to a known Resource.
Collection Interval: 30 min
Peg Condition: Based upon the SysMetric.
Measurement Scope: Server
Recovery: No action required.

CAPeakDataFIFOQueueUtil
Measurement Group: ComAgent Performance
Measurement Type: Max
Measurement Dimension: Arrayed
Description: Maximum percentage of ComAgent DataFIFO Queue Utilization.
Collection Interval: 30 min
**Peg Condition:** The maximum ComAgent DataFIFO Queue utilization sample taken during the collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement is primarily intended to assist in evaluating any issues with ComAgent User Data StackEvent processing and thread scheduling.
   
   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. Contact *My Oracle Support (MOS)* for assistance.

**CAPeakMxFIFOQueueUtil**

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Arrayed
- **Description:** Maximum percentage of ComAgent MxFIFO Queue Utilization.
- **Collection Interval:** 30 min
- **Peg Condition:** The maximum ComAgent connection MxFIFO Queue utilization sample taken during the collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement is primarily intended to assist in evaluating any issues with internal StackEvent processing and thread scheduling.
   
   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. Contact *My Oracle Support (MOS)* for assistance.

**CAPeakQueueUtil**

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed
- **Description:** Maximum percentage of Queue Utilization.
**Collection Interval:** 30 min

**Peg Condition:** The maximum ComAgent Egress Task Queue utilization sample taken during the collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

3. Contact *My Oracle Support (MOS)* for assistance.

**CAPeakRsrcPoolUtil**

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Maximum percentage of internal resource pool utilization.

**Collection Interval:** 30 min

**Peg Condition:** This is to track the measure of maximum usage of the internal resource (Ex: CommMessage Resource pool) for a given interval.

**Measurement Scope:** NE, Server

**Recovery:**

This measurement is primarily intended to assist in evaluating the need for additional processing or performance capacity tuning on a node.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of a node over several collection intervals, then the internal engineering resource pool capacity or other dependent parameters may need to be tuned, so that it does not result in unaccounted latency.

**CAPeakRxStackEvents**

- **Measurement Group:** ComAgent Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Maximum Number of User Data ingress events received.

**Collection Interval:** 30 min

**Peg Condition:** The maximum User Data ingress StackEvent sample taken during the collection interval.
Measurements

Measurement Scope: NE, Server
Recovery:
  No action required.
  This value provides a measure of Peak Value during the interval, for number of User Data messages received from remote.

CAPeakTxStackEvents
  Measurement Group: ComAgent Performance
  Measurement Type: Max
  Measurement Dimension: Single
  Description: Maximum Number of User Data egress events received from stacks to deliver it to remote.
  Collection Interval: 30 min
  Peg Condition: The maximum User Data egress StackEvent sample taken during the collection interval.
  Measurement Scope: NE, Server
  Recovery:
    No action required.
    This value provides a measure of Peak Value during the interval, for number of User Data messages transmitted to remote.

CARSTx
  Measurement Group: ComAgent Performance
  Measurement Type: Simple
  Measurement Dimension: Arrayed (by Service ID)
  Description: Number of stack events submitted to a Routed Service for routing.
  Collection Interval: 30 min
  Peg Condition: Stack event submitted to ComAgent Routed Service by a local User Layer
  Measurement Scope: Server
  Recovery:
    No action necessary

CARx
  Measurement Group: ComAgent Performance
  Measurement Type: Simple
  Measurement Dimension: Single
Measurements

Description: Number of User Data ingress events received from a peer server.
Collection Interval: 30 min
Peg Condition: For each User Data StackEvent received from one of the configured peer and processed by Communication Agent Stack.
Measurement Scope: NE, Server
Recovery: No action required.

This value provides a measure of how many User Data ingress messages are received by Communication Agent to be transmitted to local hosting stack.
This measurement count should be equal to the summation of User Data ingress events success and all User Data ingress events discards measurement counts

CARxBundled

Measurement Group: ComAgent Performance
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of ComAgent Bundled events received by ComAgent
Peg Condition: Each time a ComAgent Bundled event is received by ComAgent
Collection Interval: 30 min
Measurement Scope: Site
Recovery: No action required

CARxEventsBundled

Measurement Group: ComAgent Performance
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of stackevents received in ComAgent Bundled events
Peg Condition: Each time a stackevent is received in ComAgent Bundled events
Collection Interval: 30 min
Measurement Scope: Site
Recovery: No action required
CARxSuccess

**Measurement Group:** ComAgent Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of User Data ingress events successfully routed to local layers.  
**Collection Interval:** 30 min  
**Peg Condition:** For each User Data StackEvent received from a peer server and successfully transmitted to the local stack.  
**Measurement Scope:** NE, Server  
**Recovery:**  
  No action required.  
  This value provides a measure of how many User Data ingress messages are received by Communication Agent and are successfully transmitted to local hosting stack.

CATransEndAbnorm

**Measurement Group:** ComAgent Exception, ComAgent Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Number of reliable transactions that terminated abnormally.  
**Collection Interval:** 30 min  
**Peg Condition:**  
- Transaction times-out waiting for a response, and the maximum number of transmits has been reached.  
- Transaction time-to-live limit is exceeded.  
- Transaction terminated due to lack of resources.  
**Note:** This measurement is NOT pegged for these conditions:  
- Transaction involves an unknown service.  
- Transaction involves an unregistered Routed Service.  
**Measurement Scope:** Server  
**Recovery:**  
1. Check the ComAgent Exception report to further diagnose the reasons why transactions are failing.  
2. Contact *My Oracle Support (MOS)* for assistance.
CATransEndAbnormRateAvg

**Measurement Group:** ComAgent Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Average rate per second that ComAgent transactions ended abnormally during the collection interval.  
**Collection Interval:** 30 min  
**Peg Condition:** Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.  
**Measurement Scope:** Server  
**Recovery:**  
This measurement provides the average rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.  
No action necessary.

CATransEndAbnormRateMax

**Measurement Group:** ComAgent Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Arrayed (by Service ID)  
**Description:** Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.  
**Collection Interval:** 30 min  
**Peg Condition:** Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.  
**Measurement Scope:** Server  
**Recovery:**  
This measurement provides the maximum rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.  
No action necessary.

CATransEndNorm

**Measurement Group:** ComAgent Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Service ID)
Measurements

**Description:** Number of reliable transactions initiated by local User Layers that ended normally with a response from a destination server.

**Collection Interval:** 30 min

**Peg Condition:** When a valid reliable response stack event (G=1, A=1) is received that corresponds to a pending transaction record.

**Measurement Scope:** Server

**Recovery:**

No action necessary.

This measurement has value when compared against other measurements. If no new transactions are started, then during normal operation, this measurement should match $CATransStarted$.

**CATransPendingAvg**

**Measurement Group:** ComAgent Performance

**Measurement Type:** Average

**Measurement Dimension:** Arrayed (by Service ID)

**Description:** Average number of allocated pending transaction records over the collection interval.

**Collection Interval:** 30 min

**Peg Condition:** Average number of allocated pending transaction records during the collection interval.

**Measurement Scope:** Server

**Recovery:**

No action necessary.

**CATransPendingMax**

**Measurement Group:** ComAgent Performance

**Measurement Type:** Max

**Measurement Dimension:** Arrayed (by Service ID)

**Description:** Maximum number of allocated pending transaction records.

**Collection Interval:** 30 min

**Peg Condition:** When a pending transaction record is allocated, and the total count of allocated pending transaction records exceeds the current peak.

**Measurement Scope:** Server

**Recovery:**

No action necessary.
CATransRateAvg

Measurement Group: ComAgent Performance
Measurement Type: Average
Measurement Dimension: Arrayed (by Service ID)
Description: Average rate per second that ComAgent transactions were started during the collection interval.
Collection Interval: 30 min
Peg Condition: Transaction rate monitoring is an average rate using an exponential smoothing algorithm. The average transaction rate is a running average, smoothed over approximately 10 seconds.
Measurement Scope: Server
Recovery:
This measurement provides the average rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransRateMax

Measurement Group: ComAgent Performance
Measurement Type: Max
Measurement Dimension: Arrayed (by Service ID)
Description: Maximum rate per second that ComAgent transactions were started during the collection interval.
Collection Interval: 30 min
Peg Condition: Transaction rate monitoring is an average rate using an exponential smoothing algorithm. The average transaction rate is a running average, smoothed over approximately 10 seconds.
Measurement Scope: Server
Recovery:
This measurement provides the maximum rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransStarted

Measurement Group: ComAgent Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Service ID)
Description: Number of reliable transactions initiated by local User Layers.
Collection Interval: 30 min

Peg Condition: When a valid reliable request stack event (G=1, R=1) is received from a local User Layer.

Measurement Scope: Server

Recovery:
   No action necessary.

CATransTimeAvg

Measurement Group: ComAgent Performance
Measurement Type: Average
Measurement Dimension: Arrayed (by Service ID)
Description: Average transaction life-time in milliseconds.
Collection Interval: 30 min
Peg Condition: Transaction ends either normally or abnormally.
Measurement Scope: Server
Recovery:
   No action necessary.

CATransTimeMax

 Measurement Group: ComAgent Performance
Measurement Type: Max
Measurement Dimension: Arrayed (by Service ID)
Description: Maximum transaction life-time in milliseconds.
Collection Interval: 30 min
Peg Condition: Transaction ends either normally or abnormally.
Measurement Scope: Server
Recovery:
   No action necessary.

CATx

 Measurement Group: ComAgent Performance
Measurement Type: Simple
Measurement Dimension: Single
**Description:** Number of User Data egress events received on Communication Agent task queue from local stacks to deliver it to a peer server.

**Collection Interval:** 30 min

**Peg Condition:** For each User Data egress StackEvent received and processed by Communication Agent Stack.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of how many User Data egress messages are received by Communication Agent for direct or indirect routing service.

This measurement count should be equal to the summation of User Data egress events success and all User Data egress events discards measurement counts.

This measurement count should be equal to the summation of User Data egress events received by Communication Agent for each (Direct, Routed and HA) routing service.

---

**CATxBundled**

**Measurement Group:** ComAgent Performance

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Description:** Number of ComAgent Bundled events transmitted by ComAgent

**Peg Condition:** Each time a ComAgent Bundled event is transmitted by ComAgent

**Collection Interval:** 30 min

**Measurement Scope:** Site

**Recovery:**

No action required

---

**CATxEventsBundled**

**Measurement Group:** ComAgent Performance

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Description:** Number of stackevents transmitted through ComAgent Bundled events

**Peg Condition:** Each time a stackevent is transmitted through ComAgent Bundled events

**Collection Interval:** 30 min

**Measurement Scope:** Site

**Recovery:**
CATxSuccess

**Measurement Group:** ComAgent Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of User Data egress events successfully delivered to a peer server.

**Collection Interval:** 30 min

**Peg Condition:** For each User Data egress StackEvent transmitted to the peer server.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

This value provides a measure of how many User Data messages are successfully transmitted from hosting server to destined remote server over “event transfer” static connection.

Computer Aided Policy Making (CAPM) measurements


Table 42: CAPM Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPM_Temp_Invoked</td>
<td>Number of times a Rule Template has been invoked. This counter is incremented on a per Rule Template basis every time the Rule Template is processed.</td>
<td>5 min</td>
</tr>
<tr>
<td>CAPM_CondSet_True</td>
<td>Number of times a condition set has been evaluated to True. This counter is incremented on a per Rule Template basis every time all the conditions of the condition set match.</td>
<td>5 min</td>
</tr>
<tr>
<td>CAPM_Action_Set_Fails</td>
<td>Number of times a failure has occurred while executing the action set. This counter is incremented on a per Rule Template basis every time some of the actions fails. Note: This counter is incremented only once even if several actions within an action set have failed.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPM_MsgCopyTriggered</td>
<td>Number of times the MsgCopy action has been invoked successfully</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**CAPM_Temp_Invoked**

**Measurement Group:** CAPM  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Mediation Rule Template ID)  
**Description:** Indicates the number of times a Rule Template has been invoked. This counter is incremented on a per Rule Template basis every time the Rule Template is processed.  
**Collection Interval:** 5 min  
**Peg Condition:** A Rule Template is invoked during the message processing.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Verify that the Rule Template was set to Test or Active state and was assigned to the correct Execution Trigger.  
2. Verify the conditions of the Rule Template were properly set and the provisioned routing or/and mediation data matches the incoming message.  
3. Verify that alarm **25000 - Rule Template failed to be updated** is not raised.

**CAPM_CondSet_True**

**Measurement Group:** CAPM  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Mediation Rule Template ID)  
**Description:** Indicates the number of times a condition set has been evaluated to True. This counter is incremented on a per Rule Template basis every time all the conditions of the condition set match.  
**Collection Interval:** 5 min  
**Peg Condition:** A Condition Set matches during the message processing.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Verify that the Rule Template was set to Test or Active state and was assigned to the correct Execution Trigger.  
2. Verify the conditions of the Rule Template were properly set and the provisioned routing or/and mediation data matches the incoming message.  
3. Also verify that the alarm **25000 - Rule Template failed to be updated** is not raised.
CAPM_Action_Set_Fails

Measurement Group: CAPM
Measurement Type: Simple
Measurement Dimension: Arrayed (by Mediation Rule Template ID)
Description: Indicates the number of times a failure has occurred while executing the action set. This counter is incremented on a per Rule Template basis every time some of the actions fail.
Note: This counter is incremented only once even if several actions within an action set have failed.
Collection Interval: 5 min
Peg Condition: At least one action within an Action Set has failed.
Measurement Scope: Server Group
Recovery:
   Verify that the actions are set correctly, there are enough system resources to perform the actions, and the actions refer to the part of the incoming message that is available.

CAPM_MsgCopyTriggered

Measurement Group: CAPM
Measurement Type: Simple
Measurement Dimension: Arrayed (by Mediation Rule Template ID)
Description: The number of times the MessageCopy action has been invoked successfully.
Collection Interval: 5 min
Peg Condition: Each time the MessageCopy action has been invoked successfully.
Measurement Scope: Server Group
Recovery:
   No action required

CAPM_RxRejectWithErrorAnswer

Measurement Group: CAPM
Measurement Type: Simple
Measurement Dimension: Arrayed
Description: The number of Request messages from a downstream peer rejected by a Local Node when an indication from mediation to send back an error answer is received
Collection Interval: 5 min
Peg Condition: When mediation indicates to send back an answer
Measurement Scope: Server Group
Recovery:
No action required.

**CAPM RxSilentDiscard**

**Measurement Group:** CAPM  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed  
**Description:** The number of Request messages from a downstream peer silently by a Local Node when an indication from mediation to discard the request is received  
**Collection Interval:** 5 min  
**Peg Condition:** When mediation indicates to silently discard the request  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**Connection Congestion measurements**

The Connection Congestion measurement report contains per-connection measurements related to Diameter Connection congestion states. Measurements in this group include:

- Congestion Level-X time duration
- Number of times entered Congestion Level-X
- Number of times Remote Busy Congestion occurred

**Table 43: Connection Congestion Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnOnsetCL1</td>
<td>The number of times the connection experienced the onset of CL1.</td>
<td>5 min</td>
</tr>
<tr>
<td>ConnOnsetCL2</td>
<td>The number of times the connection experienced the onset of CL2.</td>
<td>5 min</td>
</tr>
<tr>
<td>ConnOnsetCL3</td>
<td>The number of times the connection experienced the onset of CL3.</td>
<td>5 min</td>
</tr>
<tr>
<td>ConnOnsetCL4</td>
<td>The number of times the connection experienced the onset of CL4.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
## ConnOnsetCL1

**Measurement Group:** Connection Congestion  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the connection experienced the onset of CL1.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time the congestion level for a connection changes from CL0 to CL1  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.  
2. Check to see if the Remote Busy Abatement Timeout is too small.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvEmrCongestionOnset</td>
<td>Number of times an EMR Congestion Level was advanced</td>
<td>5 min</td>
</tr>
<tr>
<td>EvRemoteBusyCongested</td>
<td>Number of times Remote Busy Congestion occurred.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvSmoothedEmrPeak</td>
<td>Smoothed EMR Peak.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvSmoothedEmrAvg</td>
<td>Smoothed EMR Average.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRejectedConnCongestion</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node because of Diameter Connection Congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmConnInCL1</td>
<td>Total amount of time (in seconds) the connection experienced CL1.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmConnInCL2</td>
<td>Total amount of time (in seconds) the connection experienced CL2.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmConnInCL3</td>
<td>Total amount of time (in seconds) the connection experienced CL3.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmConnInCL4</td>
<td>Total amount of time (in seconds) the connection experienced CL4.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

**ConnOnsetCL2**

**Measurement Group:** Connection Congestion  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the connection experienced the onset of CL2.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time the congestion level for a connection changes from CL0 or CL1 to CL2.  
**Measurement Scope:** Server Group  
**Recovery:**
1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.  
2. Check to see if the Remote Busy Abatement Timeout is too small.  
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.  
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

**ConnOnsetCL3**

**Measurement Group:** Connection Congestion  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the connection experienced the onset of CL3.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time the congestion level for a connection changes from CL0, CL1, or CL2 to CL3  
**Measurement Scope:** Server Group  
**Recovery:**
1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.  
2. Check to see if the Remote Busy Abatement Timeout is too small.
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.

4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

**ConnOnsetCL4**

**Measurement Group:** Connection Congestion  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the connection experienced the onset of CL4.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time the congestion level for a connection changes from CL0, CL1, CL2, or CL3 to CL4.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.  
2. Check to see if the Remote Busy Abatement Timeout is too small.  
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.  
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

**EvEmrCongestionOnset**

**Measurement Group:** Connection Congestion  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Number of times an EMR Congestion Level was advanced  
**Collection Interval:** 5 min  
**Peg Condition** Each time the EMR Congestion Level is advanced  
**Measurement Scope:**  
**Recovery:**  
1. Verify the "Maximum EMR" for the connection is set sufficiently high.  
2. Verify the EMR onset/abatement thresholds are properly adjusted. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "Smoothing Factor" parameter for the connection is properly adjusted. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.

4. Verify the "EMR Abatement Timeout" for the connection is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.

5. Check to see if other connections to the adjacent Diameter Node are out of service. Adjacent Diameter nodes being out of service can cause more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.

6. Check to see if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

7. If the problem persists, contact My Oracle Support (MOS).

---

**EvRemoteBusyCongestion**

- **Measurement Group:** Connection Congestion
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** Number of times Remote Busy Congestion occurred.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time the Remote Busy Congestion Level changed from CL0 to either CL1, CL2 or CL3.
- **Measurement Scope:** Site

**Recovery:**

1. Verify the "Maximum EMR" for the connection is set sufficiently high.
2. Verify the EMR onset/abatement thresholds are properly adjusted. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "Smoothing Factor" parameter for the connection is properly adjusted. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "Remote Busy Abatement Timeout" for the connection is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Check to see if other connections to the adjacent Diameter Node are out of service. Adjacent Diameter nodes being out of service can cause more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
6. Check to see if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
7. If the problem persists, contact My Oracle Support (MOS).

---

**EvSmoothedEmrAvg**

- **Measurement Group:** Connection Congestion

E53474 Revision 01, July 2014 483
Measurement Type: Average
Measurement Dimension: Arrayed (by Connection ID)
Description: Average of the “Smoothed EMR” calculations made during the collection interval.
Collection Interval: 5 min
Peg Condition: A “Smoothed EMR” calculation St is periodically calculated (every 90ms). Each time St is calculated, then the “Average Smoothed EMR” measurement shall be updated. For example, if 3 Smoothed EMR values were calculated during the collection interval – 10, 14 and 9 respectively, then the “Average Smoothed EMR” would be: 11 ((10+14+ 9)/3)
Measurement Scope: Site
Recovery:
No action necessary.

EvSmoothedEmrPeak
Measurement Group: Connection Congestion
Measurement Type: Max
Measurement Dimension: Arrayed (by Connection ID)
Description: Peak “Smoothed EMR” calculation made during the collection interval.
Collection Interval: 5 min
Peg Condition: A “Smoothed EMR” calculation St is periodically calculated (every 90ms). If the new St exceeds any previous St-k value for the collection interval, then this measurement will be updated with the new St value. For example, if 3 Smoothed EMR values were calculated during the collection interval – 10, 14 and 9 respectively, then the “Peak Smoothed EMR” would be: 14=Max(10, 14, 9)
Measurement Scope: Site
Recovery:
No action necessary.

RxRejectedConnCongestion
Measurement Group: Connection Congestion
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: Number of Request messages from a downstream peer rejected by a Local Node because of Diameter Connection Congestion.
Collection Interval: 5 min
Peg Condition: Each time an ingress transaction is abandoned and the Routing Option Set “Connection Congestion” action is invoked.
Measurement Scope: Site
Recovery:
No action required.

TmConnInCL1

Measurement Group: Connection Congestion
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: Total amount of time (in seconds) the connection experienced CL1.
Collection Interval: 5 min
Peg Condition: A "time duration interval" is determined as follows:
The "time duration interval" starts when one of the following occurs:
• New "collection interval" for the measurement begins and the connection congestion level is CL1.
• Connection congestion level changes to CL1.
The "time duration interval" stops when one of the following occurs:
• The collection interval for the measurement ends.
• The connection congestion level changes from CL1 to another congestion level.
Measurement Scope: Server Group
Recovery:
1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact My Oracle Support (MOS) for further assistance.

TmConnInCL2

Measurement Group: Connection Congestion
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: Total amount of time (in seconds) the connection experienced CL2.
Collection Interval: 5 min
Peg Condition: A "time duration interval" is determined as follows:
The "time duration interval" starts when one of the following occurs:
New "collection interval" for the measurement begins and the connection congestion level is CL2.
Connection congestion level changes to CL2.
The "time duration interval" stops when one of the following occurs:
• The collection interval for the measurement ends.
• The connection congestion level changes from CL2 to another congestion level.

Measurement Scope: Server Group

Recovery:
1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact My Oracle Support (MOS) for further assistance.

TmConnInCL3

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time (in seconds) the connection experienced CL3.

Collection Interval: 5 min

Peg Condition: A "time duration interval" is determined as follows:
The "time duration interval" starts when one of the following occurs:
• New "collection interval" for the measurement begins and the connection congestion level is CL3.
• Connection congestion level changes to CL3.
The "time duration interval" stops when one of the following occurs:
• The collection interval for the measurement ends.
• The connection congestion level changes from CL3 to another congestion level.

Measurement Scope: Server Group

Recovery:
1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

5. Contact My Oracle Support (MOS) for further assistance.

TmConnInCL4

**Measurement Group:** Connection Congestion  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Total amount of time (in seconds) the connection experienced CL4.  
**Collection Interval:** 5 min  
**Peg Condition:** A "time duration interval" is determined as follows:  
The "time duration interval" starts when one of the following occurs:

- New "collection interval" for the measurement begins and the connection congestion level is CL4.
- Connection congestion level changes to CL4.

The "time duration interval" stops when one of the following occurs:

- The collection interval for the measurement ends.
- The connection congestion level changes from CL4 to another congestion level.

**Measurement Scope:** Server Group  

**Recovery:**

1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact My Oracle Support (MOS) for further assistance.

**Connection Exception measurements**

The Connection Exception measurement report contains measurements that provide information about exceptions and unexpected messages and events for individual SCTP/TCP connections that are not specific to the Diameter protocol.
### Table 44: Connection Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvConnCerValFail</td>
<td>The number of times a CER contained invalid or unsupported AVP or AVP value.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnCexIpChkFail</td>
<td>The Host-IP-Address AVP(s) received in a CER or CEA message from the peer did not match the actual peer connection’s IP address(es).</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnCnxFail</td>
<td>Number of times the transport connection attempt failed. This includes only unsuccessful attempts to connect to the peer; it does not include failure of established connections.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnDnsFail</td>
<td>Number of times an attempt to resolve a peer’s FQDN to an IP address via DNS failed.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnFarEndClose</td>
<td>Number of times the far end closed the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnManClose</td>
<td>Number of times the connection was manually closed via administratively Disabling the connection locally.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnPeerNumIpFail</td>
<td>The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnRelease</td>
<td>The number of times the connection was terminated based on a connection release request from DRL.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnSockInitFail</td>
<td>Number of times the socket initialization failed.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnTransFail</td>
<td>The number of times the connection was closed due to SCTP/TCP transport failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnGapAckBlocks</td>
<td>The number of gap acknowledgement blocks</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxConnRetransDataChunks</td>
<td>The number of retransmitted data chunks sent on the SCTP connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnDupPkts</td>
<td>The number of duplicate packets received on the TCP connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnRetransSegs</td>
<td>The number of retransmitted segments sent on the TCP connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnSendFail</td>
<td>Number of times the transport send failed for any message on an established connection. When this occurs, the transport connection will NOT be disconnected.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**EvConnCerValFail**

**Measurement Group:** Connection Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** CER contained invalid or unsupported AVP or AVP value.  
**Collection Interval:** 5 min  
**Peg Condition:** Inband-Security AVP value in CER was other than 0 (NO_INBAND_SECURITY).  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Disable peer’s use of inband security.  
2. If the problem persists, contact *My Oracle Support (MOS).*

**EvConnCexIpChkFail**

**Measurement Group:** Connection Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The Host-IP-Address AVP(s) received in a CER or CEA message from the peer did not match the actual peer connection’s IP address(es).  
**Collection Interval:** 5 min
Peg Condition: On receipt of CER/CEA message from the peer for which the Host-IP-Address AVP(s) received in a CER or CEA message from the peer did not match the actual peer connection’s IP address(es).

Measurement Scope: Server Group

Recovery:
1. Diagnose peer to resolve inconsistency.
2. If the problem persists, contact My Oracle Support (MOS).

EvConnCnxFail

Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Connection ID)
Description: The number of times the transport connection attempt failed. This includes only unsuccessful attempts to connect to the peer; it does not include failure of established connections.
Collection Interval: 5 min
Peg Condition: Pegged when the DSR attempts to initiate a connection to a peer and fails.
Measurement Scope: Server Group
Recovery:
1. If this measurement indicates an excessive number of failed connection attempts, check that the peer is operational, and that it is accepting connections on the SCTP/TCP listen port configured for the Peer Node.
2. Contact My Oracle Support (MOS) for assistance if needed.

EvConnDnsFail

Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Connection ID)
Description: The number of times an attempt to resolve a peer’s FQDN to an IP address via DNS failed.
Collection Interval: 5 min
Peg Condition: Pegged when a connection is closed without the peer sending a DPR.
Measurement Scope: Server Group
Recovery:
1. If this measurement indicates an excessive number of DNS resolution failures, examine the DNS configuration values to determine if the correct DNS servers are being queried.
2. Examine the DNS configuration of the configured DNS servers.
3. Contact My Oracle Support (MOS) for assistance if needed.
EvConnFarEndClose

**Measurement Group:** Connection Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the far end closed the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when the peer closes the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
If this measurement indicates an excessive number of peer disconnects, the Alarm History and measurements `RxConnDpr`, `RxConnDwr`, and `TxConnDwr` should be examined to determine the reason for the peer disconnects.

EvConnManClose

**Measurement Group:** Connection Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the connection was manually closed via administratively disabling the connection locally.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a user disables a connection from the GUI.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

EvConnPeerNumIpFail

**Measurement Group:** Connection Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.  
**Collection Interval:** 5 min  
**Peg Condition:** The peer advertised a different number of IP addresses than configured.  
**Measurement Scope:** Server Group
Recovery:
Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the Diameter > Configuration > System Options page.

EvConnRelease
Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of times the connection was terminated based on a connection release request from DRL.
Collection Interval: 5 min
Peg Condition: Pegged when a connection terminated successfully on request from DRL.
Measurement Scope: Server Group
Recovery:
No action necessary.

EvSockInitFail
Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of times the socket initialization failed.
Collection Interval: 5 min
Peg Condition: Pegged when the DSR attempts to apply the SCTP/TCP socket options to a peer connection and fails.
Measurement Scope: Server Group
Recovery:
Check the SCTP/TCP options in the Connection Configuration Set for the connection and correct them.

EvConnTransFail
Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
**Description:** The number of times the transport connection was closed due to SCTP/TCP transport failure.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a connection is closed without the peer sending a DPR.

**Measurement Scope:** Server Group

**Recovery:**

1. If this measurement indicates an excessive number of ungraceful peer disconnects the Alarm History should be examined to determine the reason for the peer disconnects.
2. Contact *My Oracle Support (MOS)* for assistance if needed.

**RxConnDupPcks**

**Measurement Group:** Connection Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of duplicate packets received on the TCP connection.

**Collection Interval:** 5 min

**Peg Condition:** When duplicate packet is received on the TCP connection.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxConnDupTsns**

**Measurement Group:** Connection Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of duplicate TSNs received on the SCTP connection.

**Collection Interval:** 5 min

**Peg Condition:** When there is a duplicate TSN received on the SCTP connection from the remote peer.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxConnGapAckBlocks**

**Measurement Group:** Connection Exception
Measurements

Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of gap acknowledgement blocks received on the SCTP connection.
Collection Interval: 5 min
Peg Condition: When there is a gap in the Peer's received subsequences of data chunks as represented by their Transport Sequence Numbers (TSNs).
Measurement Scope: Server Group
Recovery:
   No action required.

RxConnGapAckBlocks
Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of gap acknowledgement blocks received on the SCTP connection.
Collection Interval: 5 min
Peg Condition: When there is a gap in the Peer's received subsequences of data chunks as represented by their Transport Sequence Numbers (TSNs).
Measurement Scope: Server Group
Recovery:
   No action required.

TxConnRetransSegs
Measurement Group: Connection Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of retransmit segments sent on the TCP connection.
Collection Interval: 5 min
Peg Condition: When a retransmitted segment is sent on the TCP connection.
Measurement Scope: Server Group
Recovery:
   No action required.
**TxConnSendFail**

**Measurement Group:** Connection Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of times the transport send failed for any message on an established connection. When this occurs, the transport connection will NOT be disconnected.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when the DSR is unable to send a message on the connection  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If this measurement indicates an excessive number of send failures, examine the $TxConnSendBufPeak$ and $TxConnSendBufAvg$ measurements.  
2. Contact *My Oracle Support (MOS)* for assistance if needed.

**Connection Performance measurements**

The Connection Performance measurement report contains measurements that provide performance information for individual SCTP/TCP connections that are not specific to the Diameter protocol.

**Table 45: Connection Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvConnCnxSuccess</td>
<td>Number of times the transport connection was successfully established. In instances where two connections are established and one is disconnected after an election, both connection establishments are counted.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPerConnQueueCongestionChange</td>
<td>Number of times that the congestion level changed for a Connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnAvgMPS</td>
<td>Exponentially smoothed average rate in MPS on the connection. Note: This measurement will be sampled periodically and reported in the Connections Maintenance GUI as a type of KPI.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxConnMsgs</td>
<td>Number of messages received on the connection. This includes all Diameter messages, both routable and non-routable.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnOctets</td>
<td>Number of octets received on the connection. This includes Diameter payload octets for all Diameter messages, both routable and non-routable.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnPeakMPS</td>
<td>Peak rate of the exponentially smoothed average rate in MPS on the connection</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnRecvBufAvg</td>
<td>Average number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnRecvBufPeak</td>
<td>Peak number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgRateAvg</td>
<td>Average Connection Ingress Message Rate.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgRatePeak</td>
<td>Peak Connection Ingress Message Rate.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxSctpChunkMp</td>
<td>Number of SCTP data chunks received by the MP (excluding duplicates).</td>
<td>5 min</td>
</tr>
<tr>
<td>RxSctpPacketMp</td>
<td>Number of SCTP packets received by the MP (excluding duplicates).</td>
<td>5 min</td>
</tr>
<tr>
<td>TmRxMPSDelay_MaxCapacity</td>
<td>Total amount of time during the measurement reporting interval that the connection experienced delay in ingress message processing because the ingress message rate on the connection exceeded the connection’s configured Maximum Ingress MPS</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TmRxMPSDelay_SharedCapacity</td>
<td>Total amount of time during the measurement reporting interval that the connection experienced delay in ingress message processing due to no capacity available in the MP server’s shared ingress MPS pool</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnMsgs</td>
<td>Number of messages sent on the connection. This includes all Diameter messages, both routable and non-routable.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnOctets</td>
<td>Number of octets sent on the connection. This includes Diameter payload octets for all Diameter messages, both routable and non-routable.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnSendBufAvg</td>
<td>Average number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnSendBufPeak</td>
<td>Peak number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnTotalDataChunks</td>
<td>The number of total data chunks sent on the SCTP connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPerConnQueueAvg</td>
<td>Per Connection Egress Message Queue Average Utilization.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPerConnQueuePeak</td>
<td>Per Connection Egress Message Queue Peak Utilization.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
EvConnCnxSuccess

Measurement Group: Connection Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Connection ID)
Description: The number of times the transport connection was successfully established. In instances where two connections are established and one is disconnected after an election, both connection establishments are counted.
Collection Interval: 5 min
Peg Condition: Pegged when a socket connection is made, regardless of which side initiates the connection.
Measurement Scope: Server Group
Recovery:
No action required.

EvPerConnQueueCongestionChange

Measurement Group: Connection Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of times that the congestion level changed for a Per Connection Egress Queue.
Collection Interval: 5 min
Peg Condition: Each time the congestion level for a Per Connection Egress Queue was changed.
Measurement Scope: Server Group
Recovery:
1. An IP network, or Diameter peer, problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem, preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the Alarms & Events page.
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. MP server status can be monitored using the Status & Manage > Server page.
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the Status & Manage > KPIs page. 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. The ingress traffic rate of each MP can be monitored using 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.
6. If the problem persists, contact *My Oracle Support (MOS)*.

**RxConnAvgMPS**

**Measurement Group:** Connection Performance

**Measurement Type:** Average

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** Exponentially smoothed average rate in MPS on the connection.

**Note:** This measurement will be sampled periodically and reported in the Connections Maintenance GUI as a KPI.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is driven by the SysMetric.

**Measurement Scope:** Per network, per NE, per MP server

**Recovery:**

This measurement indicates the exponentially smoothed 30-second average of the ingress messages per second over the measurement reporting interval. The average rate is exponentially smoothed over a 30 second interval to help eliminate variance caused by bursts in the ingress message rate. This measurement, if reported periodically, provides a history of the ingress messaging rate for each connection.

This measurement can also be seen in near real-time by viewing the connection status screen (**Diameter** > **Maintenance** > **Connections**).

No action required.

**RxConnMsgs**

**Measurement Group:** Connection Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of messages received on the connection. This includes all Diameter messages, both routable and non-routable.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

**Measurement Scope:** Server Group

**Recovery:**

No action required.
**RxConnOctets**

**Measurement Group:** Connection Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of octets received on the connection. This includes Diameter payload octets for all Diameter messages, both routable and non-routable.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**RxConnPeakMPS**

**Measurement Group:** Connection Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Peak rate of the exponentially smoothed average rate in MPS on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is driven by the SysMetric.  
**Measurement Scope:** Per network, per NE, per MP server  
**Recovery:**  
This measurement indicates the highest average rate in ingress messages per second that was processed by the Diameter connection. In other words, this measurement shows the highest value of measurement ConnIngressAvgMPS during the measurement reporting interval.  
No action required.

**RxConnRecvBufAvg**

**Measurement Group:** Connection Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The average number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.  
**Collection Interval:** 5 min
**Peg Condition:** Periodically (currently once a second) the depth of the socket receive buffer is measured and the value used to update this measurement.

**Measurement Scope:** Server Group

**Recovery:**
1. If this measurement is at or above 80%, this may be an indication that the SCTP/TCP socket receive buffer size is too small, or that the Local Node is unable to handle the load it is presented. Increase the SCTP/TCP Socket Receive Buffer Size from the Connection Configuration Set for this connection.
2. If this does not improve the situation, consider load-sharing with other DSRs.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

**RxConnRecvBufPeak**

**Measurement Group:** Connection Performance

**Measurement Type:** Max

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The peak number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.

**Collection Interval:** 5 min

**Peg Condition:** Periodically (currently once a second) the depth of the socket receive buffer is measured and the value used to update this measurement.

**Measurement Scope:** Server Group

**Recovery:**
1. If this measurement exceeds the SCTP/TCP socket receive buffer size, this may be an indication that the SCTP/TCP socket receive buffer size is too small, or that the Local Node is unable to handle the load it is presented. Increase the SCTP/TCP Socket Receive Buffer Size from the Connection Configuration Set for this connection.
2. If this does not improve the situation, consider load-sharing with other DSRs.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

**RxMsgRateAvg**

**Measurement Group:** Connection Performance

**Measurement Type:** Average

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The average connection ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).

**Collection Interval:** 5 min

**Peg Condition:** The average of all connection ingress message rate samples taken during the collection interval.
The connection measurement is associated with the connection from which the message was received.

**Measurement Scope:** Server Group

**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)](#).

**RxMsgRatePeak**

**Measurement Group:** Connection Performance

**Measurement Type:** Max

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The peak connection ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).

**Collection Interval:** 5 min

**Peg Condition:** The maximum connection ingress message rate (messages per second) sample taken during the collection interval.

The connection measurement is associated with the connection from which the message was received.

**Measurement Scope:** Server Group

**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).*

**TmRxMPSDelay_MaxCapacity**

**Measurement Group:** Connection Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Total amount of time in milliseconds that the connection experienced delay in ingress message processing because the ingress message rate on the connection exceeded the connection’s configured Maximum Ingress MPS.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented by the denial read delay in milliseconds each time a capacity refresh request results in no additional capacity due to the connection’s maximum ingress MPS budget being exhausted.  
**Measurement Scope:** Per network, per NE, per MP server  
**Recovery:** Consistently high values in this measurement indicate that the ingress message rate on the Diameter connection may be higher than the maximum ingress MPS value the connection was configured with. When this measurement is incremented, it indicates that the per connection ingress MPS control feature is throttling its rate of reading messages from the connection. This measurement is not intended to measure how much delay is being introduced into the connection’s ingress message processing; rather it is intended to give a general idea of how often per connection ingress MPS control throttling is occurring due to exhaustion of the connection’s maximum ingress MPS capacity.  
**Note:** This measurement may also be incremented due to normal spikes in the ingress MPS rate. Therefore occasional non-zero values or low values should not cause concern. If the ingress MPS rate is truly too high, Alarm **22328 - Connection is processing a higher than normal ingress messaging rate** should also be present for the connection.  
**No action required.**

**TmRxMPSDelay_SharedCapacity**

**Measurement Group:** Connection Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Total amount of time in milliseconds that the connection experienced delay in ingress message processing due to no capacity available in the DA MP’s Shared Pool.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented by the denial read delay in milliseconds each time a capacity refresh request results in no additional capacity due to lack of shared ingress MPS capacity on the MP server that hosts the connection.
**Measurement Scope:** Per network, per NE, per MP server

**Recovery:**

Consistent non-zero values in this measurement indicate that the connection was delayed in reading a message because there was no available shared ingress MPS capacity remaining on the MP server. Connections use shared ingress MPS capacity when their maximum ingress MPS is configure higher than their reserved ingress MPS and the actual rage of ingress traffic is higher than the reserved ingress MPS value. When connections competing for shared ingress MPS capacity exhaust the MP server’s licensed capacity, the per connection ingress MPS control feature delays the connection trying to read an ingress message. When this occurs, this measurement is incremented.

When this measurement is non-zero for connections using shared capacity, it indicates that the MP server is processing ingress messaging rates near or exceeding its licensed capacity. If this measurement is only rarely non-zero, the delays are in response to spikes in the ingress messaging rate. This latter condition can generally be ignored.

This measurement is not intended to measure how much delay is being introduced into the connection’s ingress message processing; rather it is intended to give a general idea of how often per connection ingress MPS control throttling is occurring due to exhaustion of the MP server’s shared ingress MPS capacity.

Please look for alarm-id 22328 to determine if any one connection is using capacity well above its configured maximum ingress MPS rate. Note, however, that it is possible for all connections to be operating within their configured maximum ingress MPS rates, but the sum of those rates exceeds the MP servers licensed MPS capacity.

No action required.

**TXConnMsgs**

**Measurement Group:** Connection Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of messages sent on the connection. This includes all Diameter messages, both routable and non-routable.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter message is sent to the peer on the connection

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**TxConnOctets**

**Measurement Group:** Connection Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)
**Description:** The number of octets sent on the connection. This includes all Diameter messages, both routable and non-routable.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter message is sent to the peer on the connection.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

---

**TxConnSendBufAvg**

**Measurement Group:** Connection Performance

**Measurement Type:** Average

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The average number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.

**Collection Interval:** 5 min

**Peg Condition:** Periodically (currently once a second) the depth of the socket send buffer is measured and the value used to update this measurement.

**Measurement Scope:** Server Group

**Recovery:**

1. If this measurement is at or above 80%, this may be an indication that the peer is unable to handle the load it is presented with. Consider load-sharing with other Peer Nodes.
2. Contact My Oracle Support (MOS) for assistance if needed.

---

**TxConnSendBufPeak**

**Measurement Group:** Connection Performance

**Measurement Type:** Max

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The peak number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.

**Collection Interval:** 5 min

**Peg Condition:** Periodically (currently once a second) the depth of the socket send buffer is measured and the value used to update this measurement.

**Measurement Scope:** Server Group

**Recovery:**

No action required.
**TxConnTotalDataChunks**

**Measurement Group:** Connection Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of total data chunks sent on the SCTP connection.  
**Collection Interval:** 5 min  
**Peg Condition:** When data chunks are transmitted on the SCTP connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**TxPerConnQueueAvg**

**Measurement Group:** Connection Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The average Per Connection Egress Message Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all Per Connection Egress Message Queue utilization samples taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**

1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.  
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the Alarms & Events page.  
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. MP server status can be monitored using the Status & Manage > Server page.  
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the Status & Manage > KPIs page. 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. The ingress traffic rate of each MP can be monitored using 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.  
6. If the problem persists, contact My Oracle Support (MOS).
**TxPerConnQueuePeak**

**Measurement Group:** Connection Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The peak Per Connection Egress Message Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum Per Connection Egress Message Queue utilization sample taken during the collection interval.  
**Measurement Scope:** Server Group  

**Recovery:**  
1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.  
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the [Alarms & Events](#) page.  
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. MP server status can be monitored using the [Status & Manage > Server](#) page.  
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the [Status & Manage > KPIs](#) page. 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. The ingress traffic rate of each MP can be monitored using 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.  
6. If the problem persists, contact [My Oracle Support (MOS)](#).

---

**Diameter Signaling Router (DSR) Application Exception measurements**

The "DSR Application Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the DSR protocol.

**Table 46: DSR Application Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxApplRequestNoRoutes</td>
<td>Number of Request messages received from a DSR Application that could not be routed.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplUnavailable</td>
<td>Number of Request messages received for a DSR Application</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxApplUnavailableForRequest</td>
<td>Number of Request messages received for a DSR Application which could not be routed to DSR Application because it was not available.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplUnavailableForAnswer</td>
<td>Number of Answer messages received for a DSR Application which could not be routed to DSR Application because it was not available.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaFullDRLAnswerReject</td>
<td>The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCpaFullDRLRequestReject</td>
<td>The number of egress Diameter Request messages that were rejected because the DRL’s Request Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrFullDRLRequestReject</td>
<td>The average Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrFullDRLAnswerDiscard</td>
<td>The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRbarFullDRLRequestReject</td>
<td>Egress Request Messages Rejected - DRL Request Queue Full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRbarFullDRLAnswerDiscard</td>
<td>Egress Answer Messages Discarded - DRL Answer Queue Full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDGlFullDRLAnswerDiscard</td>
<td>The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxApplRequestNoRoutes**

**Measurement Group:** DSR Application Exception
**Measurements**

**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by DSR Application ID)  
**Description:** Number of Request messages received from a DSR Application that could not be routed.  
**Collection Interval:** 5 min  
**Peg Condition:** When DRL successfully receives a Request message from a DSR Application that is rejected with an Answer response because either a Peer Routing Rule was not found or implicit routing could not be invoked.  
**Measurement Scope:** Server Group  
**Recovery:**  
The DSR Application is forwarding Request messages that cannot be routed to a peer. The following problems could exist:  
- A Peer Routing Rule could be missing or incorrectly configured.  
- The DSR Application could be incorrectly configured.  
- The Request message from a downstream peer was mis-routed to the DSR.  
1. Verify the Peer Routing Rules on the following GUI screen, and make any needed corrections.  
   Diameter>Configuration>Peer Routing Rules  
2. Verify the DSR Application Id configuration on the following GUI screen, and make any needed corrections.  
   Diameter>Configuration>Application Ids

**RxApplUnavailable**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Description:** Number of Request messages received for a DSR Application that could not be routed to the DSR Application because the DSR Application was Unavailable.  
**Collection Interval:** 5 min  
**Peg Condition:** When DRL receives a Request message from a peer that matches an Application Routing Rule, but cannot be routed to the DSR Application because its Operational Status is "Unavailable".  
**Measurement Scope:** Server Group  
**Recovery:**  
The DSR Application Operational Status is "Unavailable" when one of the following conditions occurs:  
- The operator has removed the DSR Application from service (Admin State is "Disabled").  
- The DSR Application was congested when an attempt to route a Request message to the SR Application occurred.  

When a DSR Application is "Unavailable", the message will be handled as defined by the "unavailability Action" attribute for the DSR Application (see the GUI screen for the DSR Application).  
1. Verify the DSR Application Admin State on the following GUI screen:
Diameter>Maintenance>Applications

2. Verify the DSR Application "Unavailability Action" attribute configuration on the following GUI screen.

Diameter>Configuration>Application Ids

RxApplUnavailableForAnswer

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by DSR Application ID)  
**Description:** Number of Answer messages received for a DSR Application which could not be routed to DSR Application because it was not available.

**Collection Interval:** 5 min  
**Peg Condition:** When DRL receives an Answer message from a peer associated with a PTR indicating that the Answer response must be routed back to the DSR Application but cannot be routed to the DSR Application because its Operational Status is “Unavailable.”  
**Measurement Scope:** Server Group  
**Recovery:**

A DSR Application’s Operational Status is “Unavailable” when one of the following conditions occur:

- The operator has removed the DSR Application from service (Admin State is “Disabled”)
- The DSR Application was congested when an attempt to route a Request message to the DSR Application occurred.

When a DSR Application is "Unavailable", the message will be handled as defined by the "unavailability Action" attribute for the DSR Application (see the GUI screen for the DSR Application).

1. Verify the DSR Application Admin State on the following GUI screen:

Diameter>Maintenance>Applications

2. Verify the DSR Application "Unavailability Action" attribute configuration on the following GUI screen.

Diameter>Configuration>Application Ids

RxApplUnavailableForRequest

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by DSR Application ID)  
**Description:** Number of Request messages received for a DSR Application which could not be routed to DSR Application because it was not available.

**Collection Interval:** 5 min
**Peg Condition**: When DRL receives a Request message from a peer which matches a ART rule but cannot be routed to the DSR Application because its Operational Status was not “Available”.

**Measurement Scope**: Server Group

**Recovery**: A DSR Application’s Operational Status is “Unavailable” when one of the following conditions occur:

- The operator has removed the DSR Application from service (Admin State is “Disabled”)
- The DSR Application was congested when an attempt to route a Request message to the DSR Application occurred.

When a DSR Application is “Unavailable”, the message will be handled as defined by the “unavailability Action” attribute for the DSR Application (see the GUI screen for the DSR Application).

1. Verify the DSR Application Admin State on the following GUI screen:
   Diameter>Maintenance>Applications
2. Verify the DSR Application “Unavailability Action” attribute configuration on the following GUI screen.
   Diameter>Configuration>Application Ids

**TxCpaFullDRLRequestReject**

**Measurement Group**: DSR Application Exception

**Measurement Type**: Average

**Measurement Dimension**: Single

**Description**: The number of egress Diameter Request messages that were rejected because the DRL’s Request Queue was full.

**Collection Interval**: 5 min

**Peg Condition**: For each Request message discarded because the “DRL’s Request Queue” was full. Used for congestion control by DSR.

**Measurement Scope**: Server Group

**Recovery**: This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
- If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
- If the problem persists, contact *My Oracle Support (MOS)*.
**TxCpaFullDRLAnswerDiscard**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Answer message discarded because the “All-Connections Event Queue” was full. Used for congestion control by DSR.  
**Measurement Scope:** Server Group  
**Recovery:** This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.  
- If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
- If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.  
- If the problem persists, contact [My Oracle Support (MOS)](https://support.oracle.com).  

**TxFabrFullDRLRequestReject**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** The average Request Message Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all Request Message Queue utilization samples taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:** This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.
• If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MP's in the Network Element may need to be increased.
• If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
• If the problem persists, contact My Oracle Support (MOS).

**TxFabrFullDRLAnswerDiscard**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Answer message discarded because the “All-Connections Event Queue” was full.  
**Measurement Scope:** Server Group  
**Recovery:**  
This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.  
• If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MP's in the Network Element may need to be increased.  
• If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.  
• If the problem persists, contact My Oracle Support (MOS).

**TxRbarFullDRLRequestReject**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of egress Diameter Request messages that were rejected because the DRL’s Request Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** When a Request message is discarded because the DRL’s Request Queue is full.  
**Measurement Scope:** Server Group
Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
- If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
- If the problem persists, contact My Oracle Support (MOS).

**TxRbarFullDRLAnswerDiscard**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** When an Answer message is discarded because the All-Connections Event Queue is full.  
**Measurement Scope:** Server Group  

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
- If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
- If the problem persists, contact My Oracle Support (MOS).

**TxGlaFullDRLAnswerDiscard**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.
Collection Interval: 5 min

Peg Condition: Each time an Answer message is discarded because the "All-Connections Event Queue" was full.

Measurement Scope: Server Group

Recovery:
This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
- If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
- If the problem persists, contact My Oracle Support (MOS).

Diameter Signaling Router (DSR) Application Performance measurements

The "DSR Application Performance" measurement group is a set of measurements that provide performance information that is specific to the DSR protocol. These measurements will allow the user to determine how many messages are successfully forwarded and received to and from each DSR Application.

Table 47: DSR Application Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxApplAnswerFwdSuccess</td>
<td>Number of Answer messages successfully forwarded to a DSR Application</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplAnswerReceived</td>
<td>Number of Answer messages received from a DSR Application</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplRequestFwdSuccess</td>
<td>Number of Request messages successfully forwarded to a DSR Application</td>
<td>5 min</td>
</tr>
<tr>
<td>RxApplRequestReceived</td>
<td>Number of Request messages received from a DSR Application</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAnswerMsgQueueAvg</td>
<td>The average Answer Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaAnswerMsgQueuePeak</td>
<td>The peak Answer Message Queue utilization (0-100%)</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxCpaAnswerProcessed</td>
<td>The total number of Answers processed by DSR Application.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaEventMsgQueueAvg</td>
<td>The average CPA Application Event Message Queue utilization measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaEventMsgQueuePeak</td>
<td>The peak CPA Application Event Message Queue utilization measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaMsgRateAvg</td>
<td>The average DSR Application’s Message Processing rate measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaMsgRatePeak</td>
<td>The peak DSR Application’s Message Processing rate measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaRequestMsgQueueAvg</td>
<td>The average Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaRequestMsgQueuePeak</td>
<td>The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCpaRequestProcessed</td>
<td>The total number of Requests processed by DSR Application.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfRequestMsgQueuePeak</td>
<td>The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfRequestMsgQueueAvg</td>
<td>The average Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfAnswerMsgQueuePeak</td>
<td>The peak DSR Application’s Answer Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxDmiwfAnswerMsgQueueAvg</td>
<td>The average Answer Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDmiwfFullDRLRequestReject</td>
<td>The number of egress Diameter Request messages that were rejected because the DRL’s Request Queue was full</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDmiwfFullDRLAnswerDiscard</td>
<td>The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfMsgRatePeak</td>
<td>The peak DSR Application’s Message Processing rate measured during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfMsgRateAvg</td>
<td>The average DSR Application’s Message Processing rate measured during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfRequestProcessed</td>
<td>The number of Requests processed by a DSR Application during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfAnswerProcessed</td>
<td>The number of Answers processed by a DSR Application during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrMsgRateAvg</td>
<td>The average DSR Application’s Ingress Message Rate measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrMsgRatePeak</td>
<td>The peak DSR Application’s Ingress Message Rate measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrRequestMsgQueueAvg</td>
<td>The average Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrRequestMsgQueuePeak</td>
<td>The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaRequestMsgQueuePeak</td>
<td>The peak DSR Application’s Request Message Queue</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxGlaRequestMsgQueueAvg</td>
<td>The average Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaMsgRatePeak</td>
<td>The peak DSR Application's Ingress Message Rate measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaMsgRateAvg</td>
<td>The average DSR Application's Ingress Message Rate measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaRequestProcessed</td>
<td>The number of Requests processed by a DSR Application during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrRequestProcessed</td>
<td>The number of Requests processed by a DSR Application during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarMsgRateAvg</td>
<td>DSR Application Message Processing Rate</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarMsgRatePeak</td>
<td>DSR Application Message Processing Rate Peak</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarRequestMsgQueueAvg</td>
<td>DSR Application Request Message Queue Average Utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarRequestMsgQueuePeak</td>
<td>DSR Application Request Message Queue Peak Utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRbarRequestProcessed</td>
<td>Total number of Requests processed by DSR Application</td>
<td>5 min</td>
</tr>
<tr>
<td>TxApplTransSuccess</td>
<td>Number of Transactions initiated by DSR Application that successfully completed</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxApplAnswerFwdSuccess**

Measurement Group: DSR Application Performance  
Measurement Type: Simple  
Measurement Dimension: Arrayed (by DSR Application ID)  
Description: Number of Answer messages successfully forwarded to a DSR Application.  
Collection Interval: 5 min
Measurements

**Peg Condition:** When DRL successfully enqueues an Answer message on the DSR Application’s internal Message Queue.

**Measurement Scope:** Server Group

**Recovery:**
No action required.

**RxApplAnswerReceived**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by DSR Application ID)

**Description:** Number of Request messages received from a DSR Application.

**Collection Interval:** 5 min

**Peg Condition:** When DRL successfully receives a Request message from a DSR Application.

**Measurement Scope:** Server Group

**Recovery:**
No action required.

**RxApplRequestFwdSuccess**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by DSR Application ID)

**Description:** Number of Request messages successfully forwarded to a DSR Application.

**Collection Interval:** 5 min

**Peg Condition:** When DRL successfully enqueues a Request message on the DSR Application’s internal Message Queue.

**Measurement Scope:** Server Group

**Recovery:**
No action required.

**RxApplRequestReceived**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by DSR Application ID)

**Description:** Number of Request messages received from a DSR Application.
Measurements

Collection Interval: 5 min
Peg Condition: When DRL successfully receives a Request message from a DSR Application.
Measurement Scope: Server Group
Recovery: No action required.

RxCpaAnswerMsgQueueAvg
Measurement Group: DSR Application Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average Answer Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The average of all Answer Message Queue utilization samples taken during the collection interval.
Measurement Scope: Server Group
Recovery: No action required.

RxCpaAnswerMsgQueuePeak
Measurement Group: DSR Application Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak Answer Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum Answer Message Queue utilization sample taken during the collection interval.
Measurement Scope: Server Group
Recovery: No action required.

RxCpaAnswerProcessed
Measurement Group: DSR Application Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The total number of Answers processed by DSR Application.
Collection Interval: 5 min
Peg Condition: This measurement will be incremented when a Diameter Answer is received.
Measurement Scope: Server Group
Recovery: No action required.

RxCpaEventMsgQueueAvg
Measurement Group: DSR Application Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average CPA Application Event Message Queue utilization measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The average Event Message Queue utilization sample taken during the collection interval.
Measurement Scope: Network, NE, Server Group
Recovery: No action required.

RxCpaEventMsgQueuePeak
Measurement Group: DSR Application Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak CPA Application Event Message Queue utilization measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum Event Message Queue utilization sample taken during the collection interval.
Measurement Scope: Network, NE, Server Group
Recovery: No action required.
RxCpaMsgRateAvg

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** The average DSR Application’s Message Processing rate measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all message processing rate samples taken during the collection interval. Used for congestion control by DSR.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxCpaMsgRatePeak

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** The peak DSR Application’s Message Processing rate measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum message processing rate sample taken during the collection interval. Used for congestion control by DSR.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxCpaRequestMsgQueueAvg

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** The average Request Message Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all Request Message Queue utilization samples taken during the collection interval.
**Measurements**

**Measurement Scope:** Server Group

**Recovery:**
No action required.

---

**RxCPaRequestMsgQueuePeak**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Max

**Measurement Dimension:** Single

**Description:** The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** The maximum Request Message Queue utilization sample taken during the collection interval.

**Measurement Scope:** Server Group

**Recovery:**
No action required.

---

**RxCPaRequestProcessed**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The total number of Requests processed by DSR Application.

**Collection Interval:** 5 min

**Peg Condition:** This measurement will be incremented when a Diameter Request is received.

**Measurement Scope:** Server Group

**Recovery:**
No action required.

---

**RxDMiWFRequestMsgQueuePeak**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Max

**Description:** The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.

**Collection Interval:** 5 min
Peg Condition: The maximum Request Message Queue utilization sample taken during the collection interval.

Measurement Scope: Server Group

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 Routing Rules
2. If no additional congestion alarms are asserted, the DSR Application Task may be experiencing a problem preventing it from processing messages from its Request Message Queue. Examine the Alarm log in Alarms & Events.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxDmiwfRequestMsgQueueAvg

Measurement Group: DSR Application Performance
Measurement Type: Average
Description: The average Request Message Queue utilization (0-100%) measured during the collection interval
Collection Interval: 5 min
Peg Condition: The average of all Request Message Queue utilization samples taken during the collection interval.
Measurement Scope: Server Group

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 Routing Rules
2. If no additional congestion alarms are asserted, the DSR Application Task may be experiencing a problem preventing it from processing messages from its Request Message Queue. Examine the Alarm log in Alarms & Events.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxDmiwfAnswerMsgQueuePeak

Measurement Group: DSR Application Performance
Measurement Type: Max
Description: The maximum Answer Message Queue utilization (0-100%) taken during the collection interval
Collection Interval: 5 min
Peg Condition: The maximum Answer Message Queue utilization sample taken during the collection interval.
Measurement Scope: Server Group

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 Routing Rules.

2. If no additional congestion alarms are asserted, the DSR Application Task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. Examine the Alarm log in Alarms & Events.

3. Contact My Oracle Support (MOS) for assistance if needed.

---

**RxDmiwfAnswerMsgQueueAvg**

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Average
- **Description:** The average of all Answer Message Queue utilization samples taken during the collection interval
- **Collection Interval:** 5 min
- **Peg Condition:** The average of all Answer Message Queue utilization samples taken during the collection interval.
- **Measurement Scope:** Server Group

**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 Routing Rules.

2. If no additional congestion alarms are asserted, the DSR Application Task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. Examine the Alarm log in Alarms & Events.

3. Contact My Oracle Support (MOS) for assistance if needed.

---

**TxDmiwfFullDRLRequestReject**

- **Measurement Group:** DSR Application Exception
- **Measurement Type:** Simple
- **Description:** The number of egress Diameter Request messages that were rejected because the DRL’s Request Queue was full.
- **Collection Interval:** 5 min
- **Peg Condition:** For each Request message discarded because the DRL’s Request Queue was full.
- **Measurement Scope:** Server Group

**Recovery:**

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
• If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
• If the problem persists, contact the My Oracle Support (MOS) for assistance.

**TxDmiwfFullDRLAnswerDiscard**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Description:** The number of egress Diameter Answer messages that were discarded because the DRL’s Answer Queue was full  
**Collection Interval:** 5 min  
**Peg Condition:** For each Answer message discarded because the All-Connections Event Queue was full  
**Measurement Scope:** Server Group  
**Recovery:**  
This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occuring.  
• If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
• If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.  
• If the problem persists, contact the My Oracle Support (MOS) for assistance.

**RxDmiwfMsgRatePeak**

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Max  
**Description:** The peak DSR Application’s Ingress Message Rate measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum DSR Application Ingress Message Rate sample taken during the collection interval.  
**Measurement Scope:** Server Group  
**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 Routing Rules
2. There may be an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored 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. Contact My Oracle Support (MOS) for assistance if needed.

**RxDmiwfMsgRateAvg**

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Average  
**Description:** The average DSR Application’s Ingress Message Rate measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all DSR Application Ingress Message Rate samples taken during the collection interval  
**Measurement Scope:** Server Group  
**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 Routing Rules  
2. There may be an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored 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. Contact My Oracle Support (MOS) for assistance if needed.

**RxDmiwfRequestProcessed**

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Simple  
**Description:** The number of Requests processed by a DSR Application during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Request message successfully de-queued from the DSR Application’s Request Message queue  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**RxDmiwfAnswerProcessed**

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Simple  
**Description:** The number of Answers processed by a DSR Application during the collection interval
Collection Interval: 5 min

Peg Condition: For each Answer message successfully de-queued from the DSR Application’s Answer Message queue

Measurement Scope: Server Group

Recovery:
  No action required.

RxFabrMsgRateAvg

Measurement Group: DSR Application Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average DSR Application’s Ingress Message Rate measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The average of all DSR Application Ingress Message Rate samples taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. Verify the configuration using Diameter > Configuration > Application Routing Rules.
   The Application Routing Table may be mis-configured and sending too much traffic to the DSR Application.
2. Use Main Menu > Status & Manage > KPIs to monitor the ingress traffic rate of each MP.
   The MPs may be unable to handle the network load. MPs are in a congestion state when the ingress message rate to the MP is exceeding its capacity to process the messages.
3. If the problem persists, contact My Oracle Support (MOS).

RxFabrMsgRatePeak

Measurement Group: DSR Application Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak DSR Application’s Ingress Message Rate measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum DSR Application Ingress Message Rate sample taken during the collection interval.
Measurement Scope: Server Group
Recovery:

1. Verify the configuration using Diameter > Configuration > Application Routing Rules. The Application Routing Table may be mis-configured and sending too much traffic to the DSR Application.

2. Use Main Menu > Status & Manage > KPIs to monitor the ingress traffic rate of each MP. The MPs may be unable to handle the network load. MPs are in a congestion state when the ingress message rate to the MP is exceeding its capacity to process the messages.

3. If the problem persists, contact My Oracle Support (MOS).

RxFabrRequestMsgQueueAvg

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** The average Request Message Queue utilization (0-100%) measured during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** The average of all Request Message Queue utilization samples taken during the collection interval.
- **Measurement Scope:** Server Group

Recovery:

1. Display and monitor the DSR Application status by selecting Diameter>Maintenance>Applications. 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 Routing Rules.

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, contact My Oracle Support (MOS).

RxFabrRequestMsgQueuePeak

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min

**Peg Condition:** The maximum Request Message Queue utilization sample taken during the collection interval.

**Measurement Scope:** Server Group

**Recovery:**

1. Display and monitor the DSR Application status by selecting Diameter>Maintenance>Applications. 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 Routing Rules.

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, contact My Oracle Support (MOS).

**RxFabrRequestProcessed**

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of Requests processed by a DSR Application during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** For each Request message successfully de-queued from the DSR Application’s Request Message queue.

**Measurement Scope:** Server Group

**Recovery:**

- No action required.

**RxGlaMsgRateAvg**

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** The average DSR Application’s Ingress Message Rate measured during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** The average of all DSR Application Ingress Message Rate samples taken during the collection interval.
**Measurements**

**Measurement Scope:** Server Group

**Recovery:**

1. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: **Diameter > Configuration > Application Routing Rules**

2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored 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. Contact **My Oracle Support (MOS)** for further assistance.

**RxGlaMsgRatePeak**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Max

**Measurement Dimension:** Single

**Description:** The peak DSR Application's Ingress Message Rate measured during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** The maximum DSR Application Ingress Message Rate sample taken during the collection interval.

**Measurement Scope:** Server Group

**Recovery:**

1. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: **Diameter > Configuration > Application Routing Rules**

2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored 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. Contact **My Oracle Support (MOS)** for further assistance.

**RxGlaRequestMsgQueueAvg**

**Measurement Group:** DSR Application Performance

**Measurement Type:** Average

**Measurement Dimension:** Single

**Description:** The average Request Message Queue utilization (0-100%) measured during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** The average of all Request Message Queue utilization samples taken during the collection interval.

**Measurement Scope:** Server Group
Recovery:
1. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: Diameter > Configuration > Application Routing Rules
2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored 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. Contact My Oracle Support (MOS) for further assistance.

RxGlaRequestMsgQueuePeak

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single

**Description:** The peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval.

- **Collection Interval:** 5 min
- **Peg Condition:** The maximum Request Message Queue utilization sample taken during the collection interval.

**Measurement Scope:** Server Group

Recovery:
1. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: Diameter > Configuration > Application Routing Rules
2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored 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. Contact My Oracle Support (MOS) for further assistance.

RxGlaRequestProcessed

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single

**Description:** The number of Requests processed by a DSR Application during the collection interval.

- **Collection Interval:** 5 min
- **Peg Condition:** Each time a Request message successfully de-queued from the DSR Application’s Request Message queue.

**Measurement Scope:** Server Group

Recovery:

No action required.

**RxRbarMsgRateAvg**

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** Average DSR Application’s Ingress Message Rate measured during the collection interval  
**Collection Interval:** 5 min  
**Peg Condition:** When the average of all DSR Application Ingress Message Rate samples is taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Display and monitor the DSR Application message rate by selecting **Diameter > Maintenance > Applications.** Verify that the message rate is set as expected.  
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 Routing Rules.**  
3. There might be an insufficient number of MPs configured to handle the network load. Monitor the traffic rate of each MP by selecting **Diameter > 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, contact **My Oracle Support (MOS).**

**RxRbarMsgRatePeak**

**Measurement Group:** DSR Application Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** Peak DSR Application’s Ingress Message Rate measured during the collection interval  
**Collection Interval:** 5 min  
**Peg Condition:** When the maximum DSR Application Ingress Message Rate sample is taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Display and monitor the DSR Application message rate by selecting **Diameter > Maintenance > Applications.** Verify that the message rate is set as expected.  
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 Routing Rules.**  
3. There might be an insufficient number of MPs configured to handle the network load. Monitor the traffic rate of each MP by selecting **Diameter > 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, contact My Oracle Support (MOS).

**RxRbarRequestMsgQueueAvg**

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** Average Request Message Queue utilization (0-100%) measured during the collection interval
- **Collection Interval:** 5 min
- **Peg Condition:** When the average of all Request Message Queue utilization samples is taken during the collection interval.

**Measurement Scope:** Server Group

**Recovery:**

1. Display and monitor the DSR Application status by selecting **Diameter > Maintenance > Applications.** Verify that the Operational Reason, which indicates congestion level, 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 Routing Rules.**

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, contact My Oracle Support (MOS).

**RxRbarRequestMsgQueuePeak**

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** Peak DSR Application’s Request Message Queue utilization (0-100%) measured during the collection interval
- **Collection Interval:** 5 min
- **Peg Condition:** When the maximum Request Message Queue utilization sample is taken during the collection interval.

**Measurement Scope:** Server Group

**Recovery:**

1. Display and monitor the DSR Application status by selecting **Diameter > Maintenance > Applications.** Verify that the Operational Reason, which indicates congestion level, 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 Routing Rules.

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, contact My Oracle Support (MOS).

### RxRbarRequestProcessed

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of Requests processed by a DSR Application during the collection interval
- **Collection Interval:** 5 min
- **Peg Condition:** When a Request message is successfully de-queued from the DSR Application’s Request Message queue.
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

### TxApplTransSuccess

- **Measurement Group:** DSR Application Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by DSR Application ID)
- **Description:** Number of Request messages received from a DSR Application.
- **Collection Interval:** 5 min
- **Peg Condition:** When DRL successfully receives a Request message from a DSR Application.
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

### Diameter Egress Transaction measurements

The Diameter Egress Transaction measurement report contains measurements providing information about Diameter peer-to-peer transactions forwarded to upstream peers.
### Table 48: Diameter Egress Transaction Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxAnswerExpectedAll</td>
<td>Number of valid Answer messages received from an upstream peer that were associated with a pending transaction.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerMsgQueueFullDiscard</td>
<td>The number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswerTimeout</td>
<td>Number of times that an Answer response was not received from a peer before the maximum allowed time PENDING_ANSWER_TIMER.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnAnswerMsgs</td>
<td>Number of routable Answer messages successfully sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnectionFailed</td>
<td>Egress peer-to-peer transactions aborted by a Local Node - connection failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnRequestMsgs</td>
<td>Number of routable Request messages successfully sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRequestSuccessAllConn</td>
<td>Number of Request messages successfully routed to a peer.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxAnswerExpectedAll**

**Measurement Group:** Diameter Egress Transaction, Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction is found.  

The connection measurement is associated with the connection from which the Answer message was received.  
**Measurement Scope:** Server Group
Recovery:

No action required.

RxAnswerMsgQueueFullDiscard

**Measurement Group:** Diameter Egress Transaction, Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Answer message discarded because the Answer Message Queue was full. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.  
3. Contact *My Oracle Support (MOS)* for assistance if needed.

TxAnswerTimeout

**Measurement Group:** Diameter Egress Transaction  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of times that an Answer response was not received from a peer before the maximum allowed time PENDING-ANSWER-TIMER. Answer timeouts can be caused by a variety of reasons:  
• The peer associated with this connection may be experiencing congestion, causing delays in sending the Answer response.  
• IP Network congestion.  
• If the peer associated with this connection is a Diameter Relay Agent, then an upstream node from the peer may be experiencing congestion, causing delays in sending the Answer response.  
**Collection Interval:** 5 min  
**Peg Condition:** When timer PENDING-ANSWER-TIMER expires. The connection measurement is associated with the connection from which the corresponding Request message was sent.
Measurement Scope: Server Group

Recovery:
1. If the user-configurable answer response timer is set too low it can cause the timer to expire before a Answer response is received. The user-configurable value is set using the page Diameter > Configuration > System Options.
2. Contact My Oracle Support (MOS) for assistance if needed.

TxConnAnswerMsgs

Measurement Group: Diameter Egress Transaction, Diameter Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of routable Answer messages successfully sent on the connection.
Collection Interval: 5 min
Peg Condition: Pegged when a Diameter Answer message is sent to the peer.

Measurement Scope: Server Group
Recovery:
No action required.

TxConnectionFailed

Measurement Group: Diameter Egress Transaction
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of times that a pending peer-to-peer transaction was abandoned due to a transport connection failure.
Collection Interval: 5 min
Peg Condition: When a pending transaction is rerouted due to a transport connection failure.
This connection measurement is associated with the connection to which the corresponding Request message was sent.

Measurement Scope: Server Group
Recovery:
1. Connection status can be monitored using the Diameter > Maintenance > Connections page.
2. Contact My Oracle Support (MOS) for assistance if needed.

TxConnRequestMsgs

Measurement Group: Diameter Egress Transaction, Diameter Performance
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of routable Request messages successfully sent on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a Diameter request message is sent to the peer.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**TxRequestSuccessAllConn**

**Measurement Group:** Diameter Egress Transaction  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of Request messages successfully routed to a peer.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR successfully queues a Request message to the DCL.  
The connection measurement is associated with the connection to which the Request message was sent.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**Diameter Exception measurements**

The Diameter Exception measurement report contains measurements that provide information about exceptions and unexpected messages and events that are specific to the Diameter protocol.

**Table 49: Diameter Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvAppIdListInconsistency</td>
<td>Number of times that the supported Application IDs received from the Peer were Inconsistent with another Transport Connection</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnCeIdValFail</td>
<td>Number of times the connection was closed due to CEA</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Realm/Host validation for locally initiated connections. Note: CER Realm/Host validation failures are tracked via the EvConnCerIdValFail measurement and are NOT included in this measurement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EvConnCexTO</td>
<td>Number of times the connection timed out waiting for the peer to send a CER or CEA.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnDpaTO</td>
<td>Number of times the connection timed out waiting for the peer to send a DPA.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnNoCommApps</td>
<td>Number of times the connection was closed due to there being no common application IDs existing between the local and peer nodes.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnPrvFail</td>
<td>Number of times the connection was closed after failing to successfully complete the proving phase.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnRejected</td>
<td>Number of times the connection was rejected. Reasons include IP address validation failure, the connection already established, and connection Administratively Disabled.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnRejInsufficientIngressMps</td>
<td>Number of times DA-MP rejected a Diameter connection due to insufficient Ingress MPS on the DA-MP to support the Reserved Ingress MPS configured for the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnRejMaxConnExceeded</td>
<td>Number of times DA-MP rejected a Diameter connection due to the DA-MP exceeding its maximum number of supported Diameter connections.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvConnWdFail</td>
<td>Number of times the Diameter Watchdog algorithm closed the connection due to no traffic received from the peer within Tw*2 time after a DWR was sent.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>EvConnWdSuspect</td>
<td>Number of times the Diameter Watchdog algorithm declared the connection suspect due to no traffic received from the peer within Tw time after a DWR was sent.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMpCerIdValFail</td>
<td>Number of times the connection was closed due to CER Realm/Host validation for peer initiated connections.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvTransLifetimeExceededMp</td>
<td>Number of transaction failures because “Transaction Lifetime” exceeded.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerMsgQueueFullDiscard</td>
<td>Number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerUnexpected</td>
<td>Number of valid Answer messages received from an upstream peer that could not be associated with a pending transaction</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnCeaError</td>
<td>Number of CEA error messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnFailMalfMsg</td>
<td>Number of messages received on the connection which were malformed. Malformed messages cause the connection to be closed.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnInvalidMsg</td>
<td>Number of messages received on the connection which had a semantic error. Messages with semantic errors are discarded.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnMpCongestionAnswerRsp</td>
<td>Number of ingress messages that were rejected with an error response because of local congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnUnexpCex</td>
<td>Number of unexpected CER/CEA messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnUnexpDpx</td>
<td>Number of unexpected DPR/DPA messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>Measurement Tag</strong></td>
<td><strong>Description</strong></td>
<td><strong>Collection Interval</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>RxConnUnexpDwx</td>
<td>Number of unexpected DWR/DWA messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMaxMpsAnswerRsp</td>
<td>The number of ingress Diameter messages that were discarded because of the MP Maximum MPS limitation and an Answer response was sent.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMaxMpsRejectMp</td>
<td>The number of ingress Diameter messages that were rejected because of MP Maximum MPS limitation and an Answer response was sent.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMpCongestionDiscardMp</td>
<td>The number of ingress Diameter Request messages received that were discarded or rejected because of local MP congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMpCongestionRejectMp</td>
<td>The number of ingress Diameter messages that were discarded because of Local MP Congestion and an Answer response was sent.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri0DiscardMp</td>
<td>The number of Green ingress Priority 0 messages discarded by the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri0DiscardMp</td>
<td>The number of Yellow ingress Priority 0 messages discarded by the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri1DiscardMp</td>
<td>The number of Green ingress Priority 1 messages discarded by the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri1DiscardMp</td>
<td>The number of Yellow ingress Priority 1 messages discarded by the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri2DiscardMp</td>
<td>The number of Green ingress Priority 2 messages discarded by the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri2DiscardMp</td>
<td>The number of Yellow ingress Priority 2 messages discarded by the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxPduPoolEmptyDiscard</td>
<td>The number of Diameter messages that were discarded because no PDU Buffers were available.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRoutableRejectMsgsMp</td>
<td>The number of ingress Diameter Request messages received that are rejected by MP with Error Answer due to MP Overload Control or Maximum IMR Limitation.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmConnDegraded</td>
<td>Total time (in seconds) during the reporting period that the connection state was in the Degraded state.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmConnEnabledNotAvail</td>
<td>Total time (in seconds) during the reporting period that the connection state was Administratively Enabled and the connection state was not Available.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAAllConnQueueFullAnswerDiscard</td>
<td>The number of egress Diameter Answer messages that were discarded because the All-Connections Event Queue was full and an Answer response was sent.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAAllConnQueueFullDiscard</td>
<td>Number of egress Diameter messages that were discarded because the All-Connections Event Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnCeaError</td>
<td>Number of CEA error messages sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnUnavailDiscard</td>
<td>Number of egress Diameter messages that were discarded by DCL because the egress connection was Unavailable.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxReqMsgApplMismatch</td>
<td>Number of times message routing detected application mismatch</td>
<td>5 min</td>
</tr>
<tr>
<td>TxReqMsgPerConnPtrMax</td>
<td>Number of times message routing bypassed the connection because the maximum allowed</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>pending transactions was exceeded</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TxRequestEgressLoop</td>
<td>Outgoing message loops detected</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**EvApplIdListInconsistency**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Number of times that the supported Application IDs received from the peer were inconsistent with another transport connection.  
**Collection Interval:** 5 min  
**Peg Condition:** If the Application ID list received from the DSR for a peer’s transport connection is not identical to the Application ID list for at least one of the transport connections for a peer that has an Operation Status state of Available.

**Measurement Scope:** Server Group  

**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 DSR may be experiencing a problem preventing it from processing events from its All-Connections Event Queue. The alarm log should be examined using the [Alarms & Events](#) page.  
5. If the problem persists, contact [My Oracle Support (MOS)](#).

**EvConnCealIdValFail**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of times the connection was closed due to CEA Realm/Host validation for locally initiated connections.
Collection Interval: 5 min

**Peg Condition:** Pegged when a CEA message is received on the connection that has an Origin-Host AVP value that does not match the FQDN configured for the peer, or an Origin-Realm AVP value that does not match the realm configured for the peer.

**Measurement Scope:** Server Group

**Recovery:**
1. Examine the Origin-Host and Origin-Realm AVP values in the CEA sent by the peer.
2. Either change the FQDN/Realm configured for the peer to match this value, or change the peer so that it sends Origin-Host/Origin-Realm AVP values that match the peer FQDN/Realm configuration.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

**EvConnCexTO**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of times the connection timed out waiting for the peer to send a CEx.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a peer initiated a connection and fails to send a CER within Tcex (from the Connection Configuration Set) seconds of the socket connection being established, or when the DSR initiates a connection and the peer fails to send a CEA within Tcex (from the Connection Configuration Set) seconds of the DSR sending a CER.

**Measurement Scope:** Server Group

**Recovery:**
1. Examine the peer to determine why it did not send the appropriate CEx message.
2. Contact *My Oracle Support (MOS)* for assistance if needed.

**EvConnDpaTO**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Connection ID)

**Description:** The number of times the connection timed out waiting for the peer to send a DPA.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a peer fails to send a DPA within Tdpx (from the Connection Configuration Set) seconds of the DSR sending a DPR.

**Measurement Scope:** Server Group

**Recovery:**
1. Examine the peer to determine why it did not respond to the DPR message that the DSR sent to it.
2. Contact My Oracle Support (MOS) for assistance if needed.

**EvConnNoCommApps**

- **Measurement Group:** Diameter Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Connection ID)
- **Description:** The number of times the connection was closed due to there being no common Application IDs existing between the Local and Peer Nodes.
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when a CEx message is received on the connection that has
  1. No Application IDs specified (when in Relay mode), or
  2. No Application IDs in common with those configured for the local node or
  3. If any of the Application IDs marked as ‘MUST exist in Peer CEx’, in the CEx Cfg Set of that connection object, is not present in the CEx message
- **Measurement Scope:** Server Group
- **Recovery:**
  Verify that either the Auth-Application-ID, the Acct-Application-ID, or the Vendor-Specific-Application-ID AVPs are present in the CEx message sent by the peer.

**EvConnPrvFail**

- **Measurement Group:** Diameter Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** The number of times the connection was closed after failing to successfully complete the proving phase.
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when a peer fails a proving period.
- **Measurement Scope:** Server Group
- **Recovery:**
  1. Examine the peer to determine why it did not respond in a timely fashion to the DWRs sent during the proving period.
  2. Consider increasing the Proving Timer in the Connection Configuration Set for the connection to allow more time for the peer to respond to DWRs.
  3. Contact My Oracle Support (MOS) for assistance if needed.
EvConnRejected

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The number of times the connection was rejected. Reasons include IP address validation failure, the connection already established, and connection administratively disabled.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a connection is rejected for any reason.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Examine the Alarm History to determine the specific reason(s) for the connection being rejected.  
2. Contact *My Oracle Support (MOS)* for assistance if needed.

EvConnRejInsufficientIngressMps

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)  
**Description:** The sum of the Reserved Ingress MPS for the added connection and MP Reserved Ingress MPS has exceeded the MP Maximum Reserved Ingress MPS. The number of times DA-MP rejected a Diameter connection due to insufficient Ingress MPS on the DA-MP to support the Reserved Ingress MPS configured for the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented for each Diameter connection that was rejected.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. The value for Reserved Ingress MPS for the added connection needs to be examined to determine if its value should be decreased.  
2. Contact *My Oracle Support (MOS)* for assistance.

EvConnRejMaxCapacityExceeded

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of times DA-MP rejected a Diameter connection due to the DA-MP exceeding its connection or ingress MPS capacity.
Collection Interval: 5 min

Peg Condition: This measurement is incremented for each Diameter connection that is rejected by a DA-MP.

Measurement Scope: Server Group

Recovery:
1. The DA-MP has reached its connection or ingress MPS capacity.
2. If the DA-MP is a member of a IPFE TS, verify that the IPFE is configured to fully monitor the DA-MP’s availability status.
   When a IPFE fully monitors application servers in a IPFE TS, it will cease from distributing new Diameter connections to any/all application servers that report a “Stasis” availability status.
3. The sum of the Reserved Ingress MPS for the added connection and MP Reserved Ingress MPS has exceeded the MP Maximum Reserved Ingress MPS. The value for Reserved Ingress MPS for the added connection needs to be examined to determine if its value should be decreased.
4. If the problem persists, contact My Oracle Support (MOS).

EvConnWdFail

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of times the Diameter watchdog algorithm closed the connection due to no traffic received from the peer within Tw*2 seconds after a DWR was sent.
Collection Interval: 5 min
Peg Condition: Pegged when no messages were received from the peer within Tw*2 seconds of sending a DWR to the peer.
Measurement Scope: Server Group
Recovery:
1. Examine the peer to determine why it is not responding to requests.
2. Contact My Oracle Support (MOS) for assistance if needed.

EvConnWdSuspect

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of times the Diameter watchdog algorithm declared the connection suspect due to no traffic received from the peer within Tw seconds after a DWR was sent.
Collection Interval: 5 min
**EvMpCerIDValFail**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of times the connection was closed due to CER Realm/Host validation for peer initiated connections.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when the value Origin-Host and/or Origin-Realm AVPs sent by the peer in its CER message do not match the values provisioned for the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Examine the Alarm History to determine the Origin Host and Realm sent by the peer.  
2. Compare these values to those configured in the Peer Node object for this connection. These values must match in order for the peer connection to be validated.  
3. Contact *My Oracle Support (MOS)* for assistance if needed.

**EvTransLifetimeExceededMp**

**Measurement Group:** DSR Application Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of transaction failures because “Transaction Lifetime” exceeded.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DRL was prevented from rerouting a Request message because the “Transaction Lifetime” was exceeded.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.
RxAnswerMsgQueueFullDiscard

**Measurement Group:** Diameter Egress Transaction, Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Answer message discarded because the Answer Message Queue was full. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.  
3. Contact *My Oracle Support (MOS)* for assistance if needed.

RxAnswerUnexpected

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction is found. The connection measurement is associated with the connection from which the Answer message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxConnCeaError

**Measurement Group:** Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of CEA error messages received on the connection.
Collection Interval: 5 min
Peg Condition: Pegged when a CEA message with a non-success response code is received on the connection.
Measurement Scope: Server Group
Recovery:
1. Examine the Alarm History to determine why the connection is being rejected.
2. Contact My Oracle Support (MOS) for assistance if needed.

RxConnFailMalfMsg

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of messages received on the connection which were malformed. Malformed messages cause the connection to be closed.
Collection Interval: 5 min
Peg Condition: Pegged when a message is received on the connection that cannot be decoded.
Measurement Scope: Server Group
Recovery:
1. Examine the Alarm History and find event 22302 - Connection Unavailable: Received malformed message for this connection.
2. Examine the displayed message bytes for errors. Monitor the connection for invalid Diameter messages.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxConnInvalidMsg

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of messages received on the connection which had a semantic error. Messages with semantic errors are discarded.
Collection Interval: 5 min
Peg Condition: Pegged when a message is received on the connection that cannot be decoded.
Measurement Scope: Server Group
Recovery:
1. Examine the Alarm History and find event 22311 - Invalid Diameter message received for this connection.
2. Examine the displayed message bytes for errors.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxConnMpCongestionAnswerRsp

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of ingress messages that were rejected with an error response because of local congestion.  
**Collection Interval:** 5 min  
**Peg Condition:** For each ingress Diameter message that was rejected because of local MP congestion and an Answer response was sent. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  

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).

RxConnOversizedMsg

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of messages received on the connection which were oversized (greater than Engineered Message Size and less than or equal to Maximum Message Size).  
**Collection Interval:** 5 min
**Peg Condition:** When the ingress message size received on the connection is greater than Engineered Message Size and less than or equal to Maximum Message Size

**Measurement Scope:** Server Group

**Recovery:**
No action required.

---

**RxConnUnexpCex**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of unexpected CER/CEA messages received on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a CER/CEA message is received on the connection after the capabilities exchange has been completed. Pegged when a CER is expected from the peer and a CEA received, or vice versa.

**Measurement Scope:** Server Group

**Recovery:**
1. Examine the Alarm History and find event 22308 - Received Unexpected CER/CEA for this connection to determine the reason that the CEx was unexpected.
2. Contact My Oracle Support (MOS) for assistance if needed.

---

**RxConnUnexpDpx**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of unexpected DPR/DPA messages received on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a DPx message is received on the connection before the capabilities exchange has been completed, or when a DPA is received without a DPR being sent to it.

**Measurement Scope:** Server Group

**Recovery:**
1. Examine the peer to determine why it is sending non-CEx messages before the capabilities exchange is complete, or why it is sending a DPA without receiving a DPR.
2. Contact My Oracle Support (MOS) for assistance if needed.
**RxConnUnexpDwx**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of unexpected DWR/DWA messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a DWx message is received on the connection before the capabilities exchange has been completed.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Examine the peer to determine why it is sending non-CEx messages before the capabilities exchange is complete.  
2. Contact *My Oracle Support (MOS)* for assistance if needed.

**RxDOCRejectConn**

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of ingress messages that were discarded because of local DA-MP danger of CPU congestion.  
**Collection Interval:** 5 min  
**Peg Condition:** For each message discarded on a connection due to DA-MP danger of CPU congestion. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed.  
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. The Diameter process may be experiencing problems. The alarm log should be examined using the Alarms & Events page.
6. If the problem persists, contact My Oracle Support (MOS).

**RxDOCRejectConn**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of ingress Diameter messages that were rejected with an error response because of local DA-MP danger of CPU congestion.  
**Collection Interval:** 5 min  
**Peg Condition:** For each message discarded on a connection with a DIAMETER (Error) Answer due to DA-MP danger of CPU congestion. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed.  
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. The Diameter process may be experiencing problems. The alarm log should be examined using the Alarms & Events page.  
6. If the problem persists, contact My Oracle Support (MOS).

**RxDOCRejectMp**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of ingress Diameter messages that were rejected with error answer due to local DA_MP danger of CPU congestion.
Collection Interval: 5 min

Peg Condition: Pegged for each message discarded with a DIAMETER (Error) Answer due to DA-MP danger of CPU congestion.

Measurement Scope: Server Group

Recovery:

1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed.

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. The Diameter process may be experiencing problems. The alarm log should be examined using the Alarms & Events page.

6. If the problem persists, contact My Oracle Support (MOS).

RxMpCongestionDiscardMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages received that were discarded or rejected because of local MP congestion.

Collection Interval: 5 min

Peg Condition: For each ingress Diameter Request message discarded because of local MP congestion.

Measurement Scope: Server Group

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).

**RxMpCongestionRejectMp**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Description:** The number of ingress messages that were rejected with error answer due to local DA-MP CPU congestion

**Collection Interval:** 5 min

**Peg Condition:** Pegged for each message discarded with a DIAMETER (Error) Answer due to a DA-MP CPU congestion.

**Measurement Scope:** Server Group

**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).

**RxMsgsOCGreenPri0DiscardMp**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of Green ingress Priority 0 messages discarded by the DA-MP Overload Control component.

**Collection Interval:** 5 min

**Peg Condition:** Each time a Priority 0 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component

**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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.

4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

**RxMsgsOCYellowPri0DiscardMp**

- **Measurement Group:** Diameter Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of Yellow ingress Priority 0 messages discarded by the DA-MP Overload Control component.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time a Priority 0 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component

**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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.

4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

**RxMsgsOCGreenPri1DiscardMp**

- **Measurement Group:** Diameter Exception
- **Measurement Type:** Simple
Measurements

Measurement Dimension: Single

Description: The number of Green ingress Priority 1 messages discarded by the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 1 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.
4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.
5. If the problem persists, contact My Oracle Support (MOS).

RxMsgsOCYellowPri1DiscardMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Yellow ingress Priority 1 messages discarded by the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 1 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu > Alarms & Events**.

5. If the problem persists, contact **My Oracle Support (MOS)**.

**RxMsgsOCGreenPri2DiscardMp**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Green ingress Priority 2 messages discarded by the DA-MP Overload Control component.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time a Priority 2 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component  
**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 DA-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 DA-MP from **Main Menu > Status & Manage > KPIs**. Each DA-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. Monitor the ingress traffic rate of each DA-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.

4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu > Alarms & Events**.

5. If the problem persists, contact **My Oracle Support (MOS)**.

**RxMsgsOCYellowPri2DiscardMp**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Yellow ingress Priority 2 messages discarded by the DA-MP Overload Control component.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time a Priority 2 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component  
**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 DA-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 DA-MP from **Main Menu > Status & Manage > KPIs**. Each DA-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. Monitor the ingress traffic rate of each DA-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.

4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu > Alarms & Events**.

5. If the problem persists, contact *My Oracle Support (MOS)*.

---

### RxPduPoolEmptyDiscard

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Diameter messages that were discarded because no PDU buffers were available.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Diameter message discarded.

The connection measurement is associated with the connection the message was received from.  
**Measurement Scope:** Server Group  
**Recovery:**

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or Diameter Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

3. Contact *My Oracle Support (MOS)* for assistance if needed.

---

### RxRoutableRejectMsgsMp

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single
**Description:** The number of ingress Diameter Request messages received that are rejected by MP with Error Answer due to MP Overload Control or Maximum IMR Limitation.

**Collection Interval:** 5 min

**Peg Condition:** Pegged for each Request message that is rejected.

**Measurement Scope:** Server Group

**Recovery:**

1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed. Contact *My Oracle Support (MOS)* for assistance.

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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.

6. If the problem persists, contact *My Oracle Support (MOS)*.

**TmConnDegraded**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** Total time (in seconds) during the reporting period that the connection state was in the Degraded state.

**Collection Interval:** 5 min

**Peg Condition:** Pegging started when a peer enters the Degraded state. Pegging stopped when the peer enters the Available or Unavailable state.

A peer may be degraded for short periods of time (< 30 seconds) due to being in a proving period or during a graceful disconnect; degraded conditions lasting longer periods of time are most likely due to local congestion.

**Measurement Scope:** Server Group

**Recovery:**

1. If this measurement indicates an excessive amount of time spent in the degraded state, examine the Alarm History to determine the cause of the degraded condition.

2. Contact *My Oracle Support (MOS)* for assistance if needed.
TmConnEnabledNotAvail

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: Total time (in seconds) during the reporting period that the connection state was administratively enabled and the connection state was not Available.
Collection Interval: 5 min
Peg Condition: Pegging is started when a peer is enabled or when a peer disconnects. Pegging is stopped when the peer connects and completes capabilities exchange, or when the connection is disabled.
Measurement Scope: Server Group
Recovery:
1. Examine the Alarm History to determine if the connection is being rejected by either end, and for notification of local congestion.
2. Make sure the peer is running.
3. If the connection is configured as a Responder connection, make sure that the peer is attempting to initiate a connection.
4. If the connection is an Initiator connection, make sure that the peer is listening on the configured port.
5. Contact My Oracle Support (MOS) for assistance if needed.

TxAllConnQueueFullDiscard

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of egress Diameter messages that were discarded because the All-Connections Event Queue was full.
Collection Interval: 5 min
Peg Condition: For each message discarded because the "All-Connections Event Queue" was full
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist
3. If the problem persists, contact My Oracle Support (MOS).
**TxConnCeaError**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of CEA error messages sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a CEA message with a non-success response code is sent on the connection.

**Measurement Scope:** Server Group

**Recovery:**
1. Examine the alarm history to determine why the connection is being rejected.
2. Contact *My Oracle Support (MOS)* for assistance if needed.

**TxConnUnavailDiscard**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of egress Diameter messages that were discarded by DCL because the egress connection was Unavailable.

**Collection Interval:** 5 min

**Peg Condition:** For each egress message discarded because the egress connection was found to be Unavailable.

**Measurement Scope:** Server Group

**Recovery:**
No action required.

**TxReqMsgApplMismatch**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of times a selected egress peer was not selected because it does not support the target Application ID in the message header.

**Collection Interval:** 5 min
**Peg Condition:** Each time the DSR bypasses a transport connection during route selection because the Application ID in the Request message does not match one of the Application IDs received from the peer on the transport connection during the Diameter Capabilities Exchange procedure. The connection measurement is associated with the egress connection to which an Application ID was not supported for routing the message.

**Measurement Scope:** Server Group

**Recovery:**
Contact *My Oracle Support (MOS)* for assistance if needed.

---

**TxReqMsgPerConnPtrMax**

**Measurement Group:** Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of times message routing bypassed the connection because the maximum allowed pending transactions was exceeded.

**Collection Interval:** 5 min

**Peg Condition:** Each time the DSR bypasses a transport connection during route selection because the maximum number of pending transactions allowed for the connection was exceeded. The connection measurement is pegged against the egress connection with the maximum number of pending transactions condition which prevented message routing.

**Measurement Scope:** Server Group

**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 DSR 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, contact *My Oracle Support (MOS)*.

---

**TxRequestEgressLoop**

**Measurement Group:** Diameter Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times that a selected route associated with an egress peer was not selected because a forwarding loop would occur (i.e., the upstream peer has already processed the Request message as determined by the Route-Record AVPs).

Collection Interval: 5 min

Peg Condition: Each time the DSR bypasses a peer during route selection because the peer’s FQDN matches one of the FQDNs in the message’s Route-Record AVPs.

The connection measurement is associated with the first connection assigned to the peer.

Note: This failure is associated with the peer, not any particular connection. The measurement should always be pegged against the same peer connection, i.e., the first one assigned to the peer.

Measurement Scope: Server Group
Recovery:

Contact My Oracle Support (MOS) for assistance if needed.

TxTestMessageDiscard

Measurement Group: Diameter Exception
Measurement Type: Simple
Measurement Dimension: Single

Description: The number of egress messages in test mode that were discarded at normal egress connection.

Collection Interval: 5 min

Peg Condition: Each time an egress message in test mode is discarded at normal egress connection

Measurement Scope: Server Group
Recovery:

Contact My Oracle Support (MOS) for assistance if needed.

Diameter Ingress Transaction Exception measurements

The Diameter Ingress Transaction Exception report group contains measurements providing information about exceptions associated with the routing of Diameter transactions received from downstream peers.
### Table 50: Diameter Ingress Transaction Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxAnsFwdFailed</td>
<td>The number of times an ingress Diameter Answer message could not be forwarded to the appropriate DA-MP, because the DA-MP was unavailable or congested.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDecodeFailure</td>
<td>Number of Request messages rejected from a downstream peer because the message could not be decoded.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiscardedMsgsPerConnControlsMp</td>
<td>Total number of ingress Diameter messages, over all connections, that were discarded by this MP. Discard is either due to the connection exceeding its configured maximum capacity, or unavailable shared capacity.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMaxMpsDiscardConn</td>
<td>Number of ingress Diameter Request messages received on a connection that were discarded because of MP Maximum MPS limitation.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMaxMpsDiscardMp</td>
<td>The number of ingress Diameter Request messages received on a connection that were discarded because of Local MP Congestion without Error Answer.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMessageLooping</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node because message looping was detected (FQDN of the Local Node associated with the ingress transport connection matched a FQDN in the messages’ Route-Record AVPs).</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMpCongestionDiscard</td>
<td>Number of ingress Diameter Request messages received on a connection that were discarded because of local MP congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxNoRoutesFound</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node because no routes were available for routing the message.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxNoRulesFailure</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node because no Peer Routing Rule was found.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPrtRuleRejection</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node because a peer routing rule ACTION is set to &quot;Send Answer&quot;.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRejectedAll</td>
<td>Number of Request messages rejected from a downstream peer by a Local Node (all reasons).</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRejectedOther</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node for any reason other than those identified by other measurements.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRequestMsgQueueFullDiscard</td>
<td>Number of ingress Diameter Request messages that were discarded because the Request Message Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRoutableDiscardedMsgsMp</td>
<td>The number of ingress Diameter Request messages received that are discarded by MP without Error Answer due to MP Overload Control or Maximum IMR Limitation.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxTransactionTimeout</td>
<td>Number of Request messages from a downstream peer rejected by a Local Node because maximum message reroutes exceeded.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxLongTimeoutPtrListEmpty</td>
<td>Number of ingress Diameter Request messages that were discarded because no Long Timeout PTR Buffers were available.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPerConnQueueFullDiscard</td>
<td>Number of egress messages that were discarded because the &quot;Per Connection Egress Message Queue&quot; was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPerConnQueueFullAnswerDiscard</td>
<td>Number of egress Answer messages that were discarded because the Per Connection Egress Message Queue was full.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxPerConnQueueFullRequestDiscard</td>
<td>Number of egress Request messages that were discarded because the Per Connection Egress Message Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPtrPoolEmpty</td>
<td>Number of ingress Diameter Request messages that were discarded because no PTR Buffers were available.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteQueueFullReject</td>
<td>Number of egress Diameter Request messages that were rejected because the Reroute Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxSockFullDiscard</td>
<td>Number of egress Diameter messages that were discarded because the socket was not writable.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

### RxAnsFwdFailed

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of times an ingress Diameter Answer message could not be forwarded to the appropriate DA-MP, because the DA-MP was unavailable or congested.  
**Collection Interval:** 5 min  
**Peg Condition:** This peg is incremented when a DA-MP receives a Diameter Answer message, identifies the DA-MP that holds the pending transaction, however finds that the DA-MP is unavailable or congested.  
**Measurement Scope:** Server Group  
**Recovery:**  
If this measurement is seen to be incrementing consistently, contact *My Oracle Support (MOS).*  
This measurement should be pegged, only when the DSR process on the destination DA-MP is Unavailable or the DA-MP is rebooting.

### RxDecodeFailure

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)
Description: Number of Request messages rejected from a downstream peer because the message could not be decoded.

Collection Interval: 5 min

Peg Condition: Request message from a downstream peer is rejected by a Local Node because it could not be decoded.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope: Server Group

Recovery:

1. These protocol violations are caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer that forwarded the message to this node (identified by the peer name) and cannot be fixed using the application.

2. Contact My Oracle Support (MOS) for assistance if needed.

**RxDiscardedMsgsPerConnControlsMp**

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of ingress Diameter messages, over all connections, that were discarded by this MP. Discard is either due to the connection exceeding its configured maximum capacity, or unavailable shared capacity.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message, received on any peer connection, is discarded due to exceeding the configured maximum ingress MPS.

Measurement Scope: Server Group

Recovery: No action required.

**RxMpCongestionDiscardConn**

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of ingress messages that were discarded because of local DA-MP CPU congestion.

Collection Interval: 5 min

Peg Condition: For each message discarded on a connection due to a DA-MP CPU congestion.

The connection measurement is associated with the connection from which the message was received.
Measurement Scope: Server Group

Recovery:

1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed.

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. The Diameter process may be experiencing problems. The alarm log should be examined using the Alarms & Events page.

6. If the problem persists, contact My Oracle Support (MOS).

RxDOCDiscardMp

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages received on a connection that were discarded due to local DA-MP danger of CPU congestion

Collection Interval: 5 min

Peg Condition: Pegged for each message discarded due to DA-MP danger of CPU congestion.

Measurement Scope: Server Group

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).
RxDOCRejectConn

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of ingress messages that were discarded because of local DA-MP danger of CPU congestion.  
**Collection Interval:** 5 min  
**Peg Condition:** For each message discarded on a connection due to DA-MP danger of CPU congestion. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed.  
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. The Diameter process may be experiencing problems. The alarm log should be examined using the [Alarms & Events](#) page.  
6. If the problem persists, contact [My Oracle Support (MOS)](#).  

RxMessageLooping

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of Request messages from a downstream peer rejected by a Local Node because message looping was detected (FQDN of the Local Node associated with the ingress transport connection matched a FQDN in the messages’ Route-Record AVPs).  
**Collection Interval:** 5 min  
**Peg Condition:** Request message from a downstream peer is rejected by a Local Node with Result-Code 3005 (DIAMETER_LOOP_DETECTED).
The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer timeouts. The status of connections should be examined from the **Diameter > Maintenance > Connections** page.
2. If no additional congestion alarms are asserted, the routing Answer task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If the problem persists, contact [My Oracle Support (MOS)](mailto:).  

**RxMpCongestionDiscardConn**

**Measurement Group:** Diameter Ingress Transaction Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of ingress Diameter Request messages received on a connection that were discarded because of local MP congestion without Error Answer.

**Collection Interval:** 5 min

**Peg Condition:** For each ingress Diameter Request message discarded because of local MP congestion. The connection measurement is associated with the connection from which the message was received.

**Measurement Scope:** Server Group

**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)](mailto:).  

**RxNoRoutesFound**

**Measurement Group:** Diameter Ingress Transaction Exception
**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** Number of Request messages from a downstream peer rejected by a Local Node because no routes were available for routing the message.

**Collection Interval:** 5 min

**Peg Condition:** Request message from a downstream peer is rejected by a Local Node because no routes were available for routing the message. A No Routes Available condition occurs when:

- A Route List was selected via a Peer Routing Rule or implicit routing but its Operational Status was Unavailable
- Implicit routing was invoked and the peer's Operational Status was not Available and an alternate implicit route was not provisioned for the peer

The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

1. If the message matched a Peer Routing Rule but none of the peers in the Route List were eligible for routing the message because either their operation state was Unavailable, the Application ID in the Request message did not match an application ID supported by the peer, or the peer had previously processed the message as defined by the Route-Record AVPs in the message:
   a) Verify that IP network connectivity exists between the MP server and the peers.
   b) Check the event history logs for additional DIAM events or alarms from this MP server.
   c) Verify that the peers in the Route List are not under maintenance. Contact [My Oracle Support (MOS)](https://oracle.com) for assistance if needed.

2. If the message was addressed to a peer directly connected to the Local Node via the Destination-Host AVP but the peer's operational status was Unavailable or the alternate path to the peer, designated by the peer's alternate implicit route was either not provisioned or was Unavailable:
   a) Verify that IP network connectivity exists between the MP server and the adjacent servers.
   b) Check the event history logs for additional DIAM events or alarms from this MP server.
   c) Verify that the peer is not under maintenance.

3. If the message was addressed to a peer directly connected to the Local Node via the Destination-Host AVP but the application ID in the Request message did not match an Application ID supported by the peer:
   a) 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](https://oracle.com) page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
   b) 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](https://oracle.com) page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
   c) 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](https://oracle.com) page.

**RxNoRulesFailure**

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of Request messages from a downstream peer rejected by a Local Node because no Peer Routing Rule was found.  
**Collection Interval:** 5 min  
**Peg Condition:** Request message from a downstream peer is rejected by a Local Node because no Peer Routing Rules were found in the peer routing table and the message was not addressed to a peer (either Destination-Host AVP was absent or Destination-Host AVP was present but was not a peer’s FQDN).  
The connection measurement is associated with the connection from which the Request message was received.  
**Measurement Scope:** Server Group  
**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 Routing 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, contact My Oracle Support (MOS).

**RxPrtRuleRejection**

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of Request messages from a downstream peer rejected by a Local Node because a Peer Routing Rule action is set to Send Answer.  
**Collection Interval:** 5 min  
**Peg Condition:** Request message from a downstream peer rejected by a Local Node because a Peer Routing Rule action is set to Send Answer.
The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxRejectedAll**

**Measurement Group:** Diameter Ingress Transaction Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of Request messages rejected from a downstream peer by a Local Node (all reasons).

**Collection Interval:** 5 min

**Peg Condition:** When measurement ID `RxRejectedConnCongestion`, `RxDecodeFailure`, `RxMessageLooping`, `RxConnInvalidMsg`, `RxNoRulesFailure`, `RxNoRoutesFound`, `RxTransactionTimeout`, `RxPrtRuleRejection`, or `RxRejectedOther` is pegged.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxRejectedOther**

**Measurement Group:** Diameter Ingress Transaction Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of Request messages from a downstream peer rejected by a Local Node for any reason other than those identified by measurements `RxDecodeFailure`, `RxMessageLooping`, `RxConnInvalidMsg`, `RxNoRulesFailure`, `RxNoRoutesFound`, `RxTransactionTimeout`, or `RxPrtRuleRejection`.

**Collection Interval:** 5 min

**Peg Condition:** Request message from a downstream peer rejected by a Local Node for any reason other than those identified by measurements `RxDecodeFailure`, `RxMessageLooping`, `RxConnInvalidMsg`, `RxNoRulesFailure`, `RxNoRoutesFound`, `RxTransactionTimeout`, or `RxPrtRuleRejection`.

The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

No action required.
**RxRequestMsgQueueFullDiscard**

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of ingress Diameter Request messages that were discarded because the Request Message Queue was full.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Request message discarded because the Request Message Queue was full. The connection measurement is associated with the connection from which the message was received.  
**Measurement Scope:** Server Group  
**Recovery:**
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.  
3. Contact *My Oracle Support (MOS)* for assistance if needed.

**RxRoutableDiscardedMsgsMp**

**Measurement Group:** Diameter Ingress Transaction Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of ingress Diameter Request messages received that are discarded by MP without Error Answer due to MP Overload Control or Maximum IMR Limitation.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when Diameter Request message is discarded.  
**Measurement Scope:** Server Group  
**Recovery:**
1. The MP is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP’s engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed. Contact *My Oracle Support (MOS)* for assistance.  
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. The Diameter process may be experiencing problems. The alarm log should be examined using the Alarms & Events page.

6. If the problem persists, contact My Oracle Support (MOS).

RxTransactionTimeout

Measurement Group: Diameter Ingress Transaction Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of Request messages from a downstream peer rejected by a Local Node because maximum message reroutes are exceeded.
Collection Interval: 5 min
Peg Condition: Request message from a downstream peer is rejected by a Local Node because maximum number of message reroutes was exceeded.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope: Server Group
Recovery:
1. If the maximum number of message reroutes is set too low (e.g., zero) then any failure trigger message reroute will fail. The user-configurable value is set using the Diameter > Configuration > System Options page.
2. If the user-configurable answer response timer is set too low the timer expires before an Answer response is received. The user-configurable value is set using the Diameter > Configuration > System Options page.
3. Contact My Oracle Support (MOS) for assistance if needed.

TxAllConnQueueFullRequestReject

Measurement Group: Diameter Ingress Transaction Exception
Measurement Type: Simple
Description: The number of egress Diameter Request messages that were rejected because the All-Connections Event Queue was full.
Collection Interval: 5 min
Peg Condition: For each Request message discarded because the All-Connections Event Queue was full.

The connection measurement is associated with the connection from which the message was received.
Measurement Scope: Server Group

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.

3. Contact My Oracle Support (MOS) for assistance if needed.

TxLongTimeoutPtrListEmpty

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Single

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages that were discarded because no Long Timeout PTR Buffers were available.

Collection Interval: 5 min

Peg Condition: When any DRL thread within the Diameter Process needs to allocate a Long Timeout PTR Buffer from the Long Timeout PTR Buffer Pool and the number of allocated Long Timeout PTRs from a Long Timeout PTR Buffer Pool is less than the maximum configured capacity of Long Timeout PTR Buffers then:

• A Long Timeout PTR Buffer shall be allocated from the Long Timeout PTR Buffer Pool
• The count for the number of allocated Long Timeout PTRs from a Long Timeout PTR Buffer Pool shall be incremented by one.

Measurement Scope: Server Group

Recovery:

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or Diameter Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

3. If the problem persists, contact My Oracle Support (MOS).

TxPerConnQueueFullDiscard

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)
Description: The number of egress messages that were discarded because the "Per Connection Egress Message Queue" was full.

Collection Interval: 5 min

Peg Condition: For each message discarded because the "Per Connection Egress Message Queue" was full

Measurement Scope: Server Group

Recovery:
1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. Examine the alarm log from Main Menu > Alarms & Events.
3. 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.
4. 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.
5. 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.
6. If the problem persists, contact My Oracle Support (MOS).

TxPerConnQueueFullAnswerDiscard

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of egress Answer messages that were discarded because the Per Connection Egress Message Queue was full.

Collection Interval: 5 min

Peg Condition: For each Per Connection Egress Message Queue Answer message discarded.

Measurement Scope: Server Group

Recovery:
1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the Alarms & Events page.
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. MP server status can be monitored using the Status & Manage > Server page.
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the Status & Manage > KPIs page. 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. The ingress traffic rate of each MP can be monitored using 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.

6. If the problem persists, contact My Oracle Support (MOS).

**TxPerConnQueueFullRequestDiscard**

**Measurement Group:** Diameter Ingress Transaction Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of egress Request messages that were discarded because the Per Connection Egress Message Queue was full.

**Collection Interval:** 5 min

**Peg Condition:** For each Per Connection Egress Message Queue Request message discarded.

**Measurement Scope:** Server Group

**Recovery:**

1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.

2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the Alarms & Events page.

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. MP server status can be monitored using the Status & Manage > Server page.

4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the Status & Manage > KPIs page. 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. The ingress traffic rate of each MP can be monitored using 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.

6. If the problem persists, contact My Oracle Support (MOS).

**TxPtrListEmpty**

**Measurement Group:** Diameter Ingress Transaction Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of ingress Diameter Request messages that were discarded because no PTR Buffers were available.
Collection Interval: 5 min

Peg Condition: When any DRL thread within the Diameter Process needs to allocate a PTR Buffer from the PTR Buffer Pool and the number of allocated PTRs from a PTR Buffer Pool is less than the maximum configured capacity of PTR Buffers then:

- A PTR Buffer shall be allocated from the PTR Buffer Pool
- The count for the number of allocated PTRs from a PTR Buffer Pool shall be incremented by one.

Measurement Scope: Server Group

Recovery:
1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or Diameter Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. Contact My Oracle Support (MOS) for assistance if needed.

TxRerouteQueueFullReject

Measurement Group: Diameter Ingress Transaction Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of egress Diameter Request messages that were rejected because the Reroute Queue was full.
Collection Interval: 5 min
Peg Condition: For each Request message rejected because the Reroute Queue was full. The connection measurement is associated with the connection the Request message was received from.
Measurement Scope: Server Group

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.
TxSockFullDiscard

Measurement Group: Diameter Ingress Transaction Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of egress Diameter messages that were discarded because the socket was not writable.
Collection Interval: 5 min
Peg Condition: For each egress Diameter message discarded because the socket was not writable.
Measurement Scope: Server Group

Recovery:
1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. Examine the alarm log from Main Menu > Alarms & Events.
3. 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.
4. 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.
5. 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.
6. If the problem persists, contact My Oracle Support (MOS).

Diameter Ingress Transaction Performance measurements

The Diameter Ingress Transaction Performance measurement report contains measurements providing information about the outcome of Diameter transactions received from downstream peers.

Table 51: Diameter Ingress Transaction Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxConnRequestMsgs</td>
<td>Number of routable Request messages received on the connection</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswer1xxx</td>
<td>Ingress Answer messages from peers successfully routed -</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>Result-Code value 1xxx (Informational)</td>
<td></td>
</tr>
<tr>
<td>TxAnswer2xxx</td>
<td>Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 2xxx (Success)</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswer3xxx</td>
<td>Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 3xxx (Protocol Error)</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswer4xxx</td>
<td>Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 4xxx (Transient Failure)</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswer5xxx</td>
<td>Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 5xxx (Permanent Failure)</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswerFailure</td>
<td>Expected Answer responses from a peer or Answer responses created by a Local Node which were not successfully routed to a downstream peer (for any reason).</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswerLocalNode</td>
<td>Answer messages created by Local Node successfully routed to downstream peers (all Result-Code values)</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswerOther</td>
<td>Answer messages from upstream peers successfully routed to downstream peers - Result-Code value not 1000-5999</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxConnRequestMsgs**

**Measurement Group:** Diameter Ingress Transaction Performance, Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of routable Request messages received on the connection.
**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter request message is received from the peer.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**TxAnswer1xxx**

**Measurement Group:** Diameter Ingress Transaction Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 1xxx.

**Collection Interval:** 5 min

**Peg Condition:** Answer message received from a peer that was successfully sent to the DSR with a Result-Code value in the range of 1000 - 1999.

The connection measurement is associated with the connection to which the message was routed.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**TxAnswer2xxx**

**Measurement Group:** Diameter Ingress Transaction Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 2xxx.

**Collection Interval:** 5 min

**Peg Condition:** Answer message received from a peer that was successfully sent to the DSR with a Result-Code value in the range of 2000 - 2999.

The connection measurement is associated with the connection to which the message was routed.

**Measurement Scope:** Server Group

**Recovery:**

No action required.
TxAnswer3xxx

Measurement Group: Diameter Ingress Transaction Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 3xxx (Protocol Error).
Collection Interval: 5 min
Peg Condition: Answer message received from a peer that was successfully sent to the DSR with a Result-Code value in the range of 3000 - 3999.
The connection measurement is associated with the connection to which the message was routed.
Measurement Scope: Server Group
Recovery: No action required.

TxAnswer4xxx

Measurement Group: Diameter Ingress Transaction Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 4xxx (Transient Failure).
Collection Interval: 5 min
Peg Condition: Answer message received from a peer that was successfully sent to the DSR with a Result-Code value in the range of 4000 - 4999.
The connection measurement is associated with the connection to which the message was routed.
Measurement Scope: Server Group
Recovery: No action required.

TxAnswer5xxx

Measurement Group: Diameter Ingress Transaction Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 5xxx (Permanent Failure).
Collection Interval: 5 min
Peg Condition: Answer message received from a peer that was successfully sent to the DSR with a Result-Code value in the range of 5000 - 5999.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope: Server Group

Recovery:

No action required.

TxAnswerFailure

Measurement Group: Diameter Ingress Transaction Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of (expected) Answer responses from a peer and Answer responses created by a Local Node which were not successfully routed to a downstream peer (for any reason).

Note: An expected Answer response from a peer is an Answer response for which a pending transaction existed.

Collection Interval: 5 min

Peg Condition: Any time the DSR fails to queue an Answer response.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope: Server Group

Recovery:

No action required.

TxAnswerLocalNode

Measurement Group: Diameter Ingress Transaction Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of Answer responses from a Local Node that were successfully routed to a downstream peer (all Result-Code values).

Collection Interval: 5 min

Peg Condition: Any time the DSR successfully creates and queues an Answer response to DCL in response to a Request message received from a downstream peer.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope: Server Group

Recovery:
No action required.

**TxAnswerOther**

**Measurement Group:** Diameter Ingress Transaction Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value not in the range of 1000-5999.  
**Collection Interval:** 5 min  
**Peg Condition:** Answer message received from a peer which was successfully sent to the DSR with either a Result-Code value not in the range of 1000 - 5999 or without a Result-Code AVP.  
The connection measurement is associated with the connection to which the message was routed.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**Diameter Performance measurements**

The Diameter Performance measurement report contains measurements that provide performance information that is specific to the Diameter protocol.

**Table 52: Diameter Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvConnPrvSuccess</td>
<td>Number of times the connection successfully completed the proving phase.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPerConnPtrQueueAvg</td>
<td>The average length of the PTR queue for a connection during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPerConnPtrQueuePeak</td>
<td>The maximum length of the PTR queue for a connection during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>RoutingMsgs</td>
<td>The number of messages processed by DRL, including Rerouting and Message Copy.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAcceptedRequestsMp</td>
<td>The number of ingress Diameter Request messages that are accepted</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxAllowedMsgsPerConnControlsMp</td>
<td>by MP to be routed after all Overload Controls are applied.</td>
<td></td>
</tr>
<tr>
<td>RxAnswerExpectedAll</td>
<td>The total number of ingress Diameter messages, over all connections, that were not discarded by MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerExpectedAllMp</td>
<td>Number of valid Answer messages received from an upstream peer that were associated with a pending transaction.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerExpectedRoutedMP</td>
<td>Number of valid Answer messages received from an upstream peer that were successfully routed to a downstream peer.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerMsgsMp</td>
<td>Number of Answer messages received.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnAnswerMsgs</td>
<td>Number of routable Answer messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnCea</td>
<td>Number of CEA messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnCer</td>
<td>Number of CER messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnDpa</td>
<td>Number of DPA messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnDpr</td>
<td>Number of DPR messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnDwa</td>
<td>Number of DWA messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnDwr</td>
<td>Number of DWR messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnOtherNonRoutable</td>
<td>Number of non-routable messages received on the connection that were not CEx, DWx, or DPx messages. Includes messages where the header P(roxy) bit is not set and messages where the application ID is 0.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxConnRequestMsgs</td>
<td>Number of routable Request messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxConnRoutableMsgs</td>
<td>Number of routable messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMaxMpsAcceptedMp</td>
<td>The number of ingress Diameter messages received that are accepted by Maximum IMR Controls of MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMaxMpsAcceptedRequestsMp</td>
<td>The number of ingress Diameter Request messages that are accepted by MP to be routed after Maximum IMR Controls are applied by MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgSize</td>
<td>Ingress message size statistics.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgSizeAvg</td>
<td>Average ingress message size in Diameter payload octets.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgSizePeak</td>
<td>Peak ingress message size in Diameter payload octets.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCPri0Mp</td>
<td>The number of ingress Priority 0 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri0Mp</td>
<td>The number of Green ingress Priority 0 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri0Mp</td>
<td>The number of Yellow ingress Priority 0 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCPri1Mp</td>
<td>The number of ingress Priority 1 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri1Mp</td>
<td>The number of Green ingress Priority 1 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri1Mp</td>
<td>The number of Yellow ingress Priority 1 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
## Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxMsgsOCPri2Mp</td>
<td>The number of ingress Priority 2 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri2Mp</td>
<td>The number of Green ingress Priority 2 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri2Mp</td>
<td>The number of Yellow ingress Priority 2 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCPri3Mp</td>
<td>The number of ingress Priority 3 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCPri0RatePeakMp</td>
<td>The peak rate of ingress Priority 0 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri0RatePeakMp</td>
<td>The peak rate of Green ingress Priority 0 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri0RatePeakMp</td>
<td>The peak rate of Yellow ingress Priority 0 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCPri1RatePeakMp</td>
<td>The peak rate of ingress Priority 1 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri1RatePeakMp</td>
<td>The peak rate of Green ingress Priority 1 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCYellowPri1RatePeakMp</td>
<td>The peak rate of Yellow ingress Priority 1 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCPri2RatePeakMp</td>
<td>The peak rate of ingress Priority 2 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgsOCGreenPri2RatePeakMp</td>
<td>The peak rate of Green ingress Priority 2 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>Measurement Tag</strong></td>
<td><strong>Description</strong></td>
<td><strong>Collection Interval</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>RxMsgsOCYellowPri2RatePeakMp</strong></td>
<td>The peak rate of Yellow ingress Priority 2 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxMsgsOCPri3RatePeakMp</strong></td>
<td>The peak rate of ingress Priority 3 messages arriving at the DA-MP Overload Control component.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxOfferedMsgsMp</strong></td>
<td>Total number of ingress Diameter messages, over all connections, offered to this MP. This includes both routable and non-routable messages.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxRequestMsgsMp</strong></td>
<td>Number of Request messages received.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxRequestNoErrors</strong></td>
<td>Transactions successfully processed on one routing attempt.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxRequestNoErrorsMp</strong></td>
<td>Number of transactions successfully processed on one routing attempt.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxRoutableAcceptedMsgsMpmn</strong></td>
<td>The number of ingress Diameter messages received that are accepted by MP for processing after all overload controls are applied.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>RxRoutableMsgsMp</strong></td>
<td>Number of routable messages received.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>TmConnAvail</strong></td>
<td>Total time in seconds that the connection state was AVAILABLE during the measurement period.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>TmConnPrvRspAvg</strong></td>
<td>Average time (in microseconds) between sending a DWR and receiving a DWA during any proving phase(s) for the measurement period. If proving fails, no sample is recorded.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>TmResponseTimeDownstream</strong></td>
<td>Average downstream transaction response time.</td>
<td>5 min</td>
</tr>
<tr>
<td><strong>TmResponseTimeDownstreamMp</strong></td>
<td>Average time (in milliseconds) from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TmResponseTimeUpstream</td>
<td>Average upstream transaction response time.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAnswerMsgsMp</td>
<td>Number of routable Answer messages transmitted.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnAnswerMsgs</td>
<td>Number of routable Answer messages successfully sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnCea</td>
<td>Number of CEA messages sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnCer</td>
<td>Number of CER messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnDpa</td>
<td>Number of DPA messages sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnDpr</td>
<td>Number of DPR messages sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnDwa</td>
<td>Number of DWA messages sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnDwr</td>
<td>Number of DWR messages received on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxConnRequestMsgs</td>
<td>Number of routable Request messages successfully sent on the connection.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgSize</td>
<td>Average egress message size in Diameter payload octets.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgSizeAvg</td>
<td>Average egress message size in Diameter payload octets.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgSizePeak</td>
<td>Peak egress message size in Diameter payload octets.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRequestMsgsMp</td>
<td>Number of routable Request messages transmitted.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRequestSuccessAllMp</td>
<td>Number of Request messages successfully routed to a peer.</td>
<td>5 min.</td>
</tr>
</tbody>
</table>

**EvConnPrvSuccess**

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Connection ID)
Measurements

Description: The number of times the connection successfully completed the proving phase.
Collection Interval: 5 min
Peg Condition: Pegged when a proving period is successfully completed.
Measurement Scope: Server Group
Recovery:

1. If the proving mode in the Connection Configuration Set is set to On Error, and this measurement indicates an excessive number of proving periods being performed, examine measurements \( \text{TxConnDpr} \), \( \text{RxConnDpa} \), \( \text{RxConnDpr} \), and \( \text{TxConnDpa} \).
2. Also examine the Alarm History for events 22303 - Connection Unavailable: Peer closed connection, 22319 - Connection Unavailable: Diameter Watchdog and 22345 - Connection Priority Level changed.
   The presence of these measurements/events may indicate that the peer is not responding to DWRs or not handling the DPx exchange on disconnect properly, after which the DSR will require a proving period.
3. Contact My Oracle Support (MOS) for assistance if needed.

EvPerConnPtrQueueAvg

- Measurement Group: Diameter Performance
- Measurement Type: Average
- Measurement Dimension: Arrayed (by Connection ID)
- Description: The average length of the PTR queue for a connection during the collection interval.
- Collection Interval: 5 min
- Peg Condition: Each time a PTR is dequeued or enqueued on the connection’s PTR queue, the average queue length is calculated using the COMCOL average measurement type method.
- Measurement Scope: Server Group
- Recovery:
   No action required.

EvPerConnPtrQueuePeak

- Measurement Group: Diameter Performance
- Measurement Type: Max
- Measurement Dimension: Arrayed (by Connection ID)
- Description: The maximum length of the PTR queue for a connection during the collection interval.
- Collection Interval: 5 min
- Peg Condition: Each time a PTR is dequeued or enqueued on the connection’s PTR queue, the maximum queue length is calculated using the COMCOL maximum measurement type method.
- Measurement Scope: Server Group
Recovery:
No action required.

RoutingMsgs

Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of messages processed by DRL, including Rerouting and Message Copy.
Collection Interval: 5 min
Peg Condition: This peg should be incremented per any of these conditions.
- Ingress Request processing resulting in the Request being routed upstream (with or without local DSR application processing of the Request)
- Ingress Answer processing resulting in forwarding of Answer downstream (with or without local DSR application processing of the Answer)
- Ingress Request processing resulting in Answer message sent by DSR to originator (with or without local DSR application processing of the Request)
- Ingress Request discarded due to validation error or overload
- Ingress Answer discarded due to validation error
- Initial copy and transmit of a Request to a DAS
- Ingress Answer triggering reroute of the pending Request message (including Answers from DAS for copied Requests)
- Request reroute due to connection failure or Answer response timeout (including reroute of copied Requests to DAS for same reasons)
- Ingress Answer from a DAS terminated by DSR due to Request copy completion or termination
Measurement Scope: Server Group

Recovery:
No action necessary.

RxAcceptedRequestsMp

Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of ingress Diameter Request messages that are accepted by MP to be routed after all Overload Controls are applied.
Collection Interval: 5 min
Peg Condition: For each message forwarded to DRI for routing
Measurement Scope: Server Group
Recovery:
No action required.

**RxAcceptedMsgsPerConnControlsMp**

- **Measurement Group:** Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The total number of ingress Diameter messages, over all connections, that were not discarded by MP
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when a Diameter message, received on any peer connection, is not discarded due to not exceeding the configured maximum ingress MPS.
- **Measurement Scope:** Server Group
- **Recovery:**
  - No action required.

**RxAnswerExpectedAll**

- **Measurement Group:** Diameter Egress Transaction, Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.
- **Collection Interval:** 5 min
- **Peg Condition:** When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction is found.

  The connection measurement is associated with the connection from which the Answer message was received.
- **Measurement Scope:** Server Group
- **Recovery:**
  - No action required.

**RxAnswerExpectedAllMp**

- **Measurement Group:** Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.
Collection Interval: 5 min
Peg Condition: When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction is found.
The connection measurement is associated with the connection from which the Answer message was received.
Measurement Scope: Server Group
Recovery: No action required.

RxAnswerExpectedRoutedMp
Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of valid Answer messages received from an upstream peer that were successfully routed to a downstream peer.
Collection Interval: 5 min
Peg Condition:
Measurement Scope: Server Group
Recovery: No action required.

RxAnswerMsgsMp
Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Answer messages received.
Collection Interval: 5 min
Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.
Measurement Scope: Server Group
Recovery: No action required.
RxConnAnswerMsgs

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of routable Answer messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a Diameter answer message is received from the peer.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxConnCea

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of CEA messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a CEA message is received on the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxConnCer

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of CER messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a CER message is received on the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.
RxConnDpa

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of DPA messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a DPA message is received on the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxConnDpr

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of DPR messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a DPR message is received on the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

RxConnDwa

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of DWA messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a DWA message is received on the connection.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.
RxConnDwr

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of DWR messages received on the connection.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a DWR message is received on the connection.  
**Measurement Scope:** Server Group  
**Recovery:** No action required.

RxConnOtherNonRoutable

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of non-routable messages received on the connection that were not CEx, DWx, or DPx messages. Includes messages where the header Proxy bit is not set and messages where the application ID is 0.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a message is received with the Proxy bit not set and the Application ID is 0, and the command code is not CEx, DWx, or DPx.  
**Note:** If this measurement is non-zero, the peer is sending commands to be processed by the Local Node that the Local Node does not understand. These messages will be discarded.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Monitor the connection to determine which messages are being addressed to the Local Node.  
2. Contact *My Oracle Support (MOS)* for assistance if needed.

RxConnRequestMsgs

**Measurement Group:** Diameter Ingress Transaction Performance, Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of routable Request messages received on the connection.  
**Collection Interval:** 5 min
**Measurements**

**Peg Condition:** Pegged when a Diameter request message is received from the peer.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxConnRoutableMsgs**

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of routable messages received on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a message with the Proxy bit set is received on the connection.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxMaxMpsAcceptedMp**

**Measurement Group:** Diameter Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single

**Description:** The number of ingress Diameter messages received that are accepted by Maximum IMR Controls of MP.

**Collection Interval:** 5 min

**Peg Condition:** Pegged for each message not discarded or rejected with "Discard Message" or "Drop Message & Send Response".

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxMaxMpsAcceptedRequestsMp**

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single
**Measurements**

**Description:** The number of ingress Diameter Request messages that are accepted by MP to be routed after Maximum IMR Controls are applied by MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time a Diameter Request message is not discarded or rejected

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxMsgSize**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Ingress message size statistics.

**Note:** Each bucket in the array contains the number of PDUs with Diameter payload octets that fell within the bucket’s range during the measurement period.

- [0] = less than 512 octets
- [1] = 512 to 1023 octets
- [2] = 1024 to 1535 octets
- [3] = 1536 to 2047 octets
- [4] = 2048 to 2559 octets
- [5] = 2560 to 3071 octets
- [6] = 3072 to 3583 octets
- [7] = 3584 to 4095 octets
- [8] = 4096 or more octets

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

**RxMsgSizeAvg**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The average ingress message size in Diameter payload octets.
**Measurements**

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

---

**RxMsgSizePeak**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The peak ingress message size in Diameter payload octets.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

**Measurement Scope:** Server Group

**Recovery:**

1. If this measurement exceeds the configured maximum Diameter message size, examine the `RxConnFailMalformedMsg` measurement to determine how many messages were discarded because of this condition.

2. Examine the Alarm History and find event **22302 - Connection Unavailable: Received malformed message** for this connection.

3. Examine the displayed message bytes for errors and monitor the connection for invalid Diameter messages.

4. Contact *My Oracle Support (MOS)* for assistance if needed.

---

**RxMsgsOCPri0Mp**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of ingress Priority 0 messages arriving at the DA-MP Overload Control component.

**Collection Interval:** 5 min

**Peg Condition:** Each time a Priority 0 Diameter Request message arrives at the DA-MP Overload Control component

**Recovery:**
No action required

RxMsgsOCGreenPri0Mp

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Green ingress Priority 0 messages arriving at the DA-MP Overload Control component.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time a Priority 0 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component  
**Recovery:**  
No action required

RxMsgsOCYellowPri0Mp

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of Yellow ingress Priority 0 messages arriving at the DA-MP Overload Control component.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time a Priority 0 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component  
**Recovery:**  
No action required

RxMsgsOCPri1Mp

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of ingress Priority 1 messages arriving at the DA-MP Overload Control component.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time a Priority 1 Diameter Request message arrives at the DA-MP Overload Control component  
**Recovery:**
No action required

**RxMsgsOCGreenPri1Mp**

Measurement Group: Diameter Performance  
Measurement Type: Simple  
Measurement Dimension: Single  
Description: The number of Green ingress Priority 1 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 1 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component  
Recovery:  
No action required

**RxMsgsOCYellowPri1Mp**

Measurement Group: Diameter Performance  
Measurement Type: Simple  
Measurement Dimension: Single  
Description: The number of Yellow ingress Priority 1 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 1 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component  
Recovery:  
No action required

**RxMsgsOCPri2Mp**

Measurement Group: Diameter Performance  
Measurement Type: Simple  
Measurement Dimension: Single  
Description: The number of ingress Priority 2 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 2 Diameter Request message arrives at the DA-MP Overload Control component  
Recovery:
No action required

RxMsgsOCGreenPri2Mp

Measurement Group: Diameter Performance  
Measurement Type: Simple  
Measurement Dimension: Single  
Description: The number of Green ingress Priority 2 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 2 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component  
Recovery:  
No action required

RxMsgsOCYellowPri2Mp

Measurement Group: Diameter Performance  
Measurement Type: Simple  
Measurement Dimension: Single  
Description: The number of Yellow ingress Priority 2 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 2 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component  
Recovery:  
No action required

RxMsgsOCPri3Mp

Measurement Group: Diameter Performance  
Measurement Type: Simple  
Measurement Dimension: Single  
Description: The number of ingress Priority 3 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 3 Diameter Request message arrives at the DA-MP Overload Control component  
Recovery:
No action required

RxMsgsOCPri0RatePeakMp

Measurement Group: Diameter Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak rate of ingress Priority 0 messages arriving at the DA-MP Overload Control component.
Collection Interval: 5 min
Peg Condition: Each time a Priority 0 Diameter Request message arrives at the DA-MP Overload Control component
Recovery: No action required

RxMsgsOCGreenPri0RatePeakMp

Measurement Group: Diameter Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak rate of Green ingress Priority 0 messages arriving at the DA-MP Overload Control component.
Collection Interval: 5 min
Peg Condition: Each time a Priority 0 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component
Recovery: No action required

RxMsgsOCYellowPri0RatePeakMp

Measurement Group: Diameter Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak rate of Yellow ingress Priority 0 messages arriving at the DA-MP Overload Control component.
Collection Interval: 5 min
Peg Condition: Each time a Priority 0 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component
Recovery:
No action required

RxMsgsOCPri1RatePeakMp

Measurement Group: Diameter Performance  
Measurement Type: Max  
Measurement Dimension: Single  
Description: The peak rate of ingress Priority 1 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 1 Diameter Request message arrives at the DA-MP Overload Control component  
Recovery: No action required

RxMsgsOCGreenPri1RatePeakMp

Measurement Group: Diameter Performance  
Measurement Type: Max  
Measurement Dimension: Single  
Description: The peak rate of Green ingress Priority 1 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 1 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component  
Recovery: No action required

RxMsgsOCYellowPri1RatePeakMp

Measurement Group: Diameter Performance  
Measurement Type: Max  
Measurement Dimension: Single  
Description: The peak rate of Yellow ingress Priority 1 messages arriving at the DA-MP Overload Control component.  
Collection Interval: 5 min  
Peg Condition: Each time a Priority 1 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component  
Recovery:
No action required

**RxMsgsOCPri2RatePeakMp**
- **Measurement Group:** Diameter Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak rate of ingress Priority 2 messages arriving at the DA-MP Overload Control component.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time a Priority 2 Diameter Request message arrives at the DA-MP Overload Control component
- **Recovery:** No action required

**RxMsgsOCGreenPri2RatePeakMp**
- **Measurement Group:** Diameter Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak rate of Green ingress Priority 2 messages arriving at the DA-MP Overload Control component.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time a Priority 2 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component
- **Recovery:** No action required

**RxMsgsOCYellowPri2RatePeakMp**
- **Measurement Group:** Diameter Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak rate of Yellow ingress Priority 2 messages arriving at the DA-MP Overload Control component.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time a Priority 2 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component
- **Recovery:**
No action required

RxMsgsOCPri3RatePeakMp

Measurement Group: Diameter Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak rate of ingress Priority 3 messages arriving at the DA-MP Overload Control component.
Collection Interval: 5 min
Peg Condition: Each time a Priority 3 Diameter Request message arrives at the DA-MP Overload Control component
Recovery:
   No action required

RxOfferedMsgsMp

Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The total number of ingress Diameter messages, over all connections, offered to this MP. This includes both routable and non-routable messages.
Collection Interval: 5 min
Peg Condition: Pegged when a Diameter message is received on any peer connection.
Measurement Scope: Server Group
Recovery:
   No action required.

RxRequestMsgsMp

Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Request messages received.
Collection Interval: 5 min
Peg Condition: Pegged when a Diameter request message received is from the peer. This measurement is pegged for all requests accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.
**Measurements**

**RxRequestNoErrors**

- **Measurement Scope**: Server Group
- **Recovery**: No action required.

**RxRequestNoErrorsMp**

- **Measurement Scope**: Server Group
- **Measurement Recovery**: No action required.

**RxRoutableAcceptedMsgsMp**

- **Measurement Scope**: Server Group
- **Measurement Recovery**: No action required.
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of ingress Diameter messages received that are accepted by MP for processing after all overload controls are applied.
Collection Interval: 5 min
Peg Condition: Pegged when Diameter message is sent to DRL for routing.
Measurement Scope: Server Group
Recovery: No action required.

RxRoutableMsgsMp
Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of routable messages received.
Collection Interval: 5 min
Peg Condition: Pegged when a Diameter message, with the Proxy bit set, is received from the peer. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.
Measurement Scope: Server Group
Recovery: No action required.

TmConnAvail
Measurement Group: Diameter Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Connection ID)
Description: Total time in seconds that the connection state was available during the measurement period.
Collection Interval: 5 min
Peg Condition: Pegging started when the connection state is Available. Pegging stopped when the connection state is Unavailable or Degraded.
Measurement Scope: Server Group
Recovery:
1. If this measurement varies significantly from the total time in the collection period, examine the Alarm History to determine the reason(s) that the connection was Unavailable or Degraded.
2. Contact My Oracle Support (MOS) for assistance if needed.

TmConnPrvRspAvg

**Measurement Group:** Diameter Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The average time (in microseconds) between sending a DWR and receiving a DWA during any proving phase(s) for the measurement period. If proving fails, no sample is recorded.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged after a proving period completes successfully.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

TmResponseTimeDownstream

**Measurement Group:** Diameter Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Average time (in milliseconds) from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer.  
**Collection Interval:** 5 min  
**Peg Condition:** Time interval for each transaction starts when the DSR successfully decodes an ingress Request message from a downstream peer. Time interval for each transaction stops when the DSR attempts to send an Answer response. This includes Answer messages received from upstream peers and those generated by the DSR. The connection measurement is associated with the connection from which the Request message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If the average is significantly larger than what is considered normal, then additional measurements, such as measurement TmResponseTimeUpstream, should be consulted to assist in determining the source of the delay.  
2. Contact My Oracle Support (MOS) for assistance if needed.

TmResponseTimeDownstreamMp

**Measurement Group:** Diameter Performance
**Measurement Type:** Average

**Measurement Dimension:** Single

**Description:** Average time (in milliseconds) from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer.

**Collection Interval:** 5 min

**Peg Condition:** Time interval for each transaction starts when the DSR successfully decodes an ingress Request message from a downstream peer. Time interval for each transaction stops when the DSR attempts to send an Answer response. This includes Answer messages received from upstream peers and those generated by the DSR.

The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

---

**TmResponseTimeUpstream**

**Measurement Group:** Diameter Performance

**Measurement Type:** Average

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** Average time (in milliseconds) from when routing forwards a Request message to an upstream peer to the time that an Answer response is received.

**Collection Interval:** 5 min

**Peg Condition:** Time interval for each transaction starts when the DSR successfully queues a Request message. Time interval for each transaction stops when the DSR receives an Answer response for the pending transaction associated with the forwarded Request message.

The connection measurement is associated with the connection the Request message is sent to.

**Note:** This measurement excludes transactions which are aborted due to a failure (E.g., timer PENDING-ANSWER-TIMER or PENDING-TRANSACTION-TIMER expiration or transport connection failure).

**Measurement Scope:** Server Group

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance if needed.

---

**TxAnswerMsgsMp**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single
Measurements

**TxConnAnswerMsgs**

- **Description:** The number of routable Answer messages transmitted.
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when a Diameter Answer message is sent to the peer on the connection.
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**TxConnCea**

- **Measurement Group:** Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** The number of CEA messages sent on the connection.
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when a CEA message is sent on the connection.
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**TxConnCer**

- **Measurement Group:** Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
Measurements

**Description:** The number of CER messages sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** When a CER message is sent to the peer on the connection. This measurement is pegged for CER messages indicating success as well as those indicating an error. A separate measurement (TxConnCerErr) is also pegged if the CER indicates an error.

**Measurement Scope:** Server Group

**Recovery:** No action required.

---

**TxConnDpa**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of DPA messages sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a DPA message is sent on the connection.

**Measurement Scope:** Server Group

**Recovery:** No action required.

---

**TxConnDpr**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of DPR messages sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a DPR message is sent on the connection.

**Measurement Scope:** Server Group

**Recovery:** No action required.

---

**TxConnDwa**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple
**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of DWA messages sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a DWA message is sent on the connection.

**Measurement Scope:** Server Group

**Recovery:**
- No action required.

---

**TxConnDwr**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of DWR messages sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a DWR message is received on the connection.

**Measurement Scope:** Server Group

**Recovery:**
- No action required.

---

**TxConnRequestMsgs**

**Measurement Group:** Diameter Egress Transaction, Diameter Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of routable Request messages successfully sent on the connection.

**Collection Interval:** 5 min

**Peg Condition:** Pegged when a Diameter request message is sent to the peer.

**Measurement Scope:** Server Group

**Recovery:**
- No action required.

---

**TxMsgSize**

**Measurement Group:** Diameter Performance

**Measurement Type:** Simple
**Measurement Dimension**: Single

**Description**: Egress message size statistics.

**Note**: Each bucket in the array contains the number of PDUs with Diameter payload octets that fell within the bucket's range during the measurement period.

- [0] = less than 512 octets
- [1] = 512 to 1023 octets
- [2] = 1024 to 1535 octets
- [3] = 1536 to 2047 octets
- [4] = 2048 to 2559 octets
- [5] = 2560 to 3071 octets
- [6] = 3072 to 3583 octets
- [7] = 3584 to 4095 octets
- [8] = 4096 or more octets

**Collection Interval**: 5 min

**Peg Condition**: Pegged when a Diameter message is sent to the peer on the connection.

**Measurement Scope**: Server Group

**Recovery**: No action required.

---

**TxMsgSizeAvg**

**Measurement Group**: Diameter Performance

**Measurement Type**: Simple

**Measurement Dimension**: Single

**Description**: The average egress message size in Diameter payload octets.

**Collection Interval**: 5 min

**Peg Condition**: Pegged when a Diameter message is sent to the peer on the connection.

**Measurement Scope**: Server Group

**Recovery**: No action required.

---

**TxMsgSizePeak**

**Measurement Group**: Diameter Performance

**Measurement Type**: Simple

**Measurement Dimension**: Single

**Description**: The peak egress message size in Diameter payload octets.

**Collection Interval**: 5 min
**Peg Condition:** Pegged when the size of the Diameter message sent to the peer is larger than any other message sent to the peer during the reporting interval.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

---

**TxRequestMsgsMp**

- **Measurement Group:** Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of routable Request messages transmitted.
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when a Diameter Request message is sent to the peer on the connection.
- **Measurement Scope:** Server Group
- **Recovery:**

No action required.

---

**TxRequestSuccessAllMP**

- **Measurement Group:** Diameter Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of Request messages successfully routed to a peer.
- **Collection Interval:** 5 min
- **Peg Condition:** When the DSR successfully queues a Request message.

The connection measurement is associated with the connection to which the Request message was sent.

- **Measurement Scope:** Server Group
- **Recovery:**

No action required.

---

**Diameter Rerouting measurements**

The Diameter Rerouting measurement report is a set of measurements which allows the user to evaluate the amount of message rerouting attempts which are occurring, the reasons for why message rerouting is occurring, and the success rate of message rerouting attempts.
## Table 53: Diameter Rerouting Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRerouteAnswerRsp</td>
<td>Answer messages received associated with rerouted Request messages</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRerouteAnswerRspMp</td>
<td>Number of valid Answer messages received from an upstream peer that were associated with a pending rerouted transaction.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteAnswerResponse</td>
<td>Number of message rerouting attempts triggered by the receipt of an Answer response Result-Code value which is a candidate for message rerouting.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteAnswerTimeout</td>
<td>Rerouting attempts triggered by a timeout on the Answer response.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteAttempts</td>
<td>Total number of message rerouting attempts.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteConnFailure</td>
<td>Rerouting attempts triggered by a connection failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteSuccessSent</td>
<td>Message rerouting attempts that were successfully rerouted.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

### RxRerouteAnswerRsp

**Measurement Group:** Diameter Rerouting  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of valid Answer messages received from an upstream peer that were associated with a pending rerouted transaction.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction associated with a rerouted message is found. The connection measurement is associated with the connection from which the Answer message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.
**RxRerouteAnswerRspMp**

**Measurement Group:** Diameter Rerouting  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of valid Answer messages received from an upstream peer that were associated with a pending rerouted transaction.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR receives an Answer message event with a valid Transport Connection ID for which a pending transaction associated with a rerouted message is found.  
The connection measurement is associated with the connection from which the Answer message was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**TxRerouteAnswerResponse**

**Measurement Group:** Diameter Rerouting  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of message rerouting attempts triggered by the receipt of an Answer response Result-Code value that is a candidate for message rerouting.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR receives an Answer response with a Result-Code value that is a candidate for message rerouting.  
The connection measurement is associated with the upstream connection from which the Answer response was received.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**TxRerouteAnswerTimeout**

**Measurement Group:** Diameter Rerouting  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)
**Description:** The number of message rerouting attempts triggered by a timeout (PENDING-ANSWER-TIMER) on the Answer response.

**Collection Interval:** 5 min

**Peg Condition:** When timer PENDING-ANSWER-TIMER expires and the DSR attempts to reroute a Request message.

**Measurement Scope:** Server Group

**Recovery:**
1. If the user-configurable answer response timer is set too low it can cause the timer to expire before a Answer response is received. The user-configurable value is set from the Diameter > Configuration > System Options page.
2. Contact My Oracle Support (MOS) for assistance if needed.

**TxRerouteAttempts**

**Measurement Group:** Diameter Rerouting

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** Total number of message rerouting attempts.

**Collection Interval:** 5 min

**Peg Condition:** When the DSR attempts to reroute a Request message routed via a Route List for one of the following reasons:
- Transport connection fails
- PENDING-ANSWER-TIMER expires
- Answer response Result-Code plus application ID matches user-defined values for message rerouting

This measurement will be pegged when any of the following measurement IDs are pegged: TxRerouteConnFailure, TxRerouteAnswerTimeout, TxRerouteAnswerResponse.

The connection measurement is associated with the upstream connection from which rerouting was triggered.

**Measurement Scope:** Server Group

**Recovery:**
1. If the user-configurable answer response timer is set too low it can cause the timer to expire before an Answer response is received. The user-configurable value is set from the Diameter > Configuration > System Options page.
2. Connection status can be monitored from the Diameter > Maintenance > Connections page.
3. Contact My Oracle Support (MOS) for assistance if needed.

**TxRerouteConnFailure**

**Measurement Group:** Diameter Rerouting

**Measurement Type:** Simple
**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of message rerouting attempts triggered by a connection failure.

**Collection Interval:** 5 min

**Peg Condition:** For each Request message rerouting attempt invoked by the receipt of a valid Connection Down event notification from the DSR.

**Measurement Scope:** Server Group

**Recovery:**

1. Connection status can be monitored from the [Diameter > Maintenance > Connections](#) page.
2. Contact [My Oracle Support (MOS)](http://mos.oracle.com) for assistance if needed.

---

**TxRerouteSuccessSent**

- **Measurement Group:** Diameter Rerouting
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** The number of message rerouting attempts that were successfully rerouted.
- **Collection Interval:** 5 min
- **Peg Condition:** When the DSR successfully reroutes a Request message.

The connection measurement is associated with the upstream connection from which rerouting was triggered.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

---

**DM-IWF Exception measurements**

The DM-IWF Exception measurement report contains measurements providing information about transaction processing exceptions that are specific to the MAP-Diameter IWF Application running on a DA-MP.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxMtoDRoutingFail</td>
<td>Number of MAP-to-Diameter transactions which could not be routed to the Diameter network due to a failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDtoMRoutingFail</td>
<td>Number of Diameter-to-MAP transactions which could not be routed to a SS7-MP due to a failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>EvDtoMtimeout</td>
<td>Number of Diameter-to-MAP transactions failures due to time-out on DA-MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDtoMReject</td>
<td>Number of Diameter-to-MAP transactions either rejected via Answer response or discarded by DM-IWF due to a failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDmiwfPtrPoolExceeded</td>
<td>Number of transactions rejected - no PTRs</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDSS7MPAnswerUnexpected</td>
<td>Number of Unexpected Answer messages received from SS7-MPs</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfSvcCongest</td>
<td>Number of Diameter-to-MAP Request messages that could not be forwarded to MD-IWF Routed Service due to service congestion</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfError</td>
<td>Number of Diameter-to-MAP Request messages forwarded to MAP Routed Service that received error notification</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfConnExhausted</td>
<td>Number of Diameter messages that could not be forwarded to MD-IWF (SS7-MP) due to failure to enqueue message to ComAgent</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDmIwfSS7MpFailure</td>
<td>Number of Diameter-to-MAP Request messages forwarded to MD-IWF Routed Service that failed to be Answered due to SS7-MP failure</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiscOnError</td>
<td>Number of Diameter messages that were discarded on error</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDmIwfTxFwdFail</td>
<td>Number of Diameter messages that could not be forwarded by DM-IWF to DRL due to DRL queue exhaustion</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDmiwfMsgSizeExceeded</td>
<td>Number of Diameter messages received from DRL that got rejected because the Diameter message exceeded supported maximum “Diameter Max Message Size”</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**TxDmiwfMtoDRoutingFail**

**Measurement Group:** DM-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** Number of MAP-to-Diameter transactions which could not be routed to the Diameter network due to a failure.
Collection Interval: 5 min

Peg Condition:

- Whenever DM-IWF is unable to successfully forward a Request message received from a SS7-MP due to a failure.
- Whenever the Request message is not routed to a Diameter Peer Node due to a routing error (either DRL or another DSR Application initiates an Answer response).
- Whenever DM-IWF receives an Answer response from DRL and the Application-Data stack event parameter "Message Source ID" is set to "DRL" or "APP".

Recovery:

1. Examine the Admin State of the DM-IWF DSR application. Verify that the DM-IWF DSR application is Enabled via the Diameter > Maintenance > Applications screen.
2. If the DM-IWF DSR application is enabled, this measurement is pegged when either DM-IWF internal resources are exhausted or DSR's internal request processing queue is highly congested. Examine the following additional information to determine which resources are exhausted and/or whether the DSR internal queue is congested:
   - Alarms and Events from the Alarms & Events screen (Alarm 33005 - DM-IWF PTR Pool Utilization)
   - Measurement EvDmiwfPtrPoolExceeded
   - Measurement EvDmIwfTxFwdFail
3. Evaluate the cause of resource exhaustion or internal queue congestion and take corrective action. Examine the following additional information to assist with determination of the cause of resource exhaustion:
   - Alarms and Events from the Alarms & Events screen
   - The rate of messages being processed by DM-IWF from the Status & Manage > KPIs page
4. If the problem persists, contact My Oracle Support (MOS).

TxDmiwfDtoMRoutingFail

Measurement Group: DM-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of Diameter-to-MAP transactions which could not be routed to a SS7-MP.
Collection Interval: 5 min
Peg Condition: Whenever DM-IWF is unable to successfully forward a Request message received from DRL to a SS7-MP due to a failure.
Recovery:

1. Examine whether DM-IWF resources are exhausted.
   - Alarms and Events from the Alarms & Events screen (Alarm 33005 - DM-IWF PTR Pool Utilization)
   - Measurement EvDmiwfPtrPoolExceeded
2. If DM-IWF resources are exhausted, evaluate the cause of resource exhaustion and take corrective action. Examine the following additional information to assist with determination of the cause of resource exhaustion
   - Alarms and Events from the Alarms & Events screen
   - The rate of messages being processed by DM-IWF from the Status & Manage > KPIs page

3. Examine whether the MAP routed service is congested, by reviewing the "MDIWFSvc" Routed Service Provider's states for via Main menu > Communication Agent > Maintenance > Routed Services Status screen. If the routed service is congested
   The number of SS7-MPs that act as providers for the MAP Routed Service might be insufficient to service the offered ingress load. Individual service provider status can be monitored from Main Menu > Communication Agent > Maintenance > Routed Services Status

4. If the problem persists, contact My Oracle Support (MOS).

**EvDmiwfDtoMtimeout**

- **Measurement Group:** DM-IWF Exception
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Description:** Number of Diameter-to-MAP transaction failures due to time-out on a DA-MP.
- **Collection Interval:** 5 min
- **Peg Condition:** Each DM-IWF abandons a Diameter-to-MAP transaction due to a DM-IWF Pending Answer Timer expiration.
- **Recovery:**
  1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. Determine if the MAP Origination Transaction Timer value is set too low via Main Menu > MAP Interworking > Configuration > Options (MF-IWF tab).
  2. If the problem persists, contact My Oracle Support (MOS).

**EvDmiwfPtrPoolExceeded**

- **Measurement Group:** DM-IWF Exception
- **Measurement Dimension:** Arrayed (by Transaction Direction)
- **Measurement Type:** Simple
- **Description:** Number of transactions rejected - no PTRs
- **Collection Interval:** 5 min
- **Peg Condition:** Each time DM-IWF fails to allocate a PTR for either a Diameter-to-MAP or MAP-to-Diameter transaction.
- **Recovery:**
  1. The maximum number of PTRs on a DA-MP is set to a default value, but may need to be increased.
  2. Contact My Oracle Support (MOS) for assistance.
RxDmiwfSS7MPAnswerUnexpected

Measurement Group: DM-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of Unexpected Answer messages received from SS7-MPs
Collection Interval: 5 min
Peg Condition: Each time an Answer message received from an MD-IWF which was discarded because the pending transaction associated with the message could not be found.
Recovery:
1. If this event is occurring frequently, the timer may be set too low. The timer value can be viewed via Main Menu > MAP Interworking > Configuration > System Options.
2. Contact My Oracle Support (MOS) for assistance.

EvMdIwfSvcCongest

Measurement Group: DM-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of Diameter-to-MAP Request messages that could not be forwarded to MD-IWF Routed Service due to service congestion.
Collection Interval: 5 min
Peg Condition: Each time DM-IWF fails to forward a Request to MD-IWF(SS7-MP) because the message priority of the Request message was less than the MD-IWF Routed Service Congestion Level.
Recovery:
1. The number of SS7-MPs that act as providers for the MD-IWF Routed Service might be insufficient to service the offered ingress load.
2. If the problem occurs frequently, contact My Oracle Support (MOS).

EvMdIwfError

Measurement Group: DM-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of Diameter-to-MAP Request messages forwarded to MAP Routed Service that received error notification.
Collection Interval: 5 min
Peg Condition: For each Request forwarded to MD-IWF that received a ComAgent Error response
Recovery:
If the problem persists, contact My Oracle Support (MOS).

EvMdIwfConnExhausted
Measurement Group: DM-IWF Exception
Measurement Dimension: Arrayed (by Message Type)
Measurement Type: Simple
Description: Number of Diameter messages that could not be forwarded to MD-IWF (SS7-MP) due to failure to enqueue message to ComAgent.
Collection Interval: 5 min
Peg Condition: For each Request forwarded to MD-IWF that received a ComAgent Error response
Recovery:
If the problem persists, contact My Oracle Support (MOS).

RxDiscOnError
Measurement Group: DM-IWF Exception
Measurement Dimension: Arrayed (by Error Condition)
Measurement Type: Simple
Description: The number of Diameter messages that were discarded on error for the error conditions:
• 0: Encode decode error, D-to-M Request
• 1: Encode decode error, D-to-M Answer
• 2: Encode decode error, M-to-D Request
• 3: Encode decode error, M-to-D Answer
Collection Interval: 5 min
Peg Condition: When a Diameter message is discarded on error
Recovery:
Contact My Oracle Support (MOS) for further assistance.

EvDmIwfTxFwdFail
Measurement Group: DM-IWF Exception
Measurement Dimension: Arrayed (by Message Type)
Measurement Type: Simple
Description: Number of Diameter messages that could not be forwarded by DM-IWF to DRL due to DRL queue exhaustion
Collection Interval: 5 min
**Peg Condition:** Any time DM-IWF fails to enqueue a Diameter message to DRL's Request or Answer Task

**Recovery:**

**Note:** This alarm should not occur unless the MP is experiencing local congestion as indicated by 22200 - Local MP Congestion, 22201 - Ingress Message Rate, 22204 - Request Message Queue Utilization, and 22205 - Answer Message Queue Utilization.

If the problem occurs frequently, contact *My Oracle Support (MOS).*

---

**EvDmiwfMsgSizeExceeded**

**Measurement Group:** DM-IWF Exception

**Measurement Dimension:** Arrayed (by Diameter Message Type - Request/Answer

**Measurement Type:** Simple

**Description:** Number of Diameter messages received from DRL that got rejected because the Diameter message size exceeded maximum "Diameter Max Message Size"

**Collection Interval:** 5 min

**Peg Condition:** Each time DM-IWF fails to forward a Diameter message to SS7-MP because its size exceeds the supported maximum

**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".

---

**DM-IWF Performance measurements**

The Diameter Interworking Function Performance measurement report contains measurements providing performance information that is specific to the MAP-Diameter IWF Application running on a DA-MP.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxDmiwfDtoMTransCnt</td>
<td>Number of Diameter-to-MAP transaction messages processed.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfDtoMTransRateAvg</td>
<td>Average number of Diameter-to-MAP transaction messages processed per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfDtoMTransRatePeak</td>
<td>Peak number of Diameter-to-MAP transaction messages processed per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfMtoDTransCnt</td>
<td>Number of MAP-to-Diameter transaction messages processed.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxDmiwfMtoDTransRateAvg</td>
<td>Average number of MAP-to-Diameter transaction messages processed per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfMtoDTransRatePeak</td>
<td>Peak number of MAP-to-Diameter transaction messages processed per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfTransactionRspQueuePeak</td>
<td>Transaction Response Queue Peak Utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfTransactionRspQueueAvg</td>
<td>Transaction Response Queue Average Utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDmiwfPtrPoolPeak</td>
<td>DM-IWF PTR Buffer Pool Peak Utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDmiwfPtrPoolAvg</td>
<td>DM-IWF PTR Buffer Pool Average Utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfRequestMessage</td>
<td>Number of Request messages with Command Code &quot;X&quot; received from DRL.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfAnswerMessage</td>
<td>Number of Answer messages with Command Code &quot;X&quot; received from DRL.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDmiwfRequestMessage</td>
<td>Number of Request messages with Command Code &quot;X&quot; successfully sent to DRL.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDmiwfAnswerMessage</td>
<td>Number of Answer messages with Command Code &quot;X&quot; successfully sent to DRL.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfRequestMessageIwf</td>
<td>Number of Request messages processed by DM-IWF that were received from an SS7-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDmiwfAnswerMessageIwf</td>
<td>Number of Answer messages processed by DM-IWF that were received from an SS7-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDmiwfRequestMessageIwf</td>
<td>Number of Request messages sent to an SS7-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>TxDmiwfAnswerMessageIwf</td>
<td>Number of Answer messages to an SS7-MP</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxDmiwfDtoMTransCnt**

**Measurement Group:** DM-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** Number of Diameter-to-MAP transaction messages processed.  
**Collection Interval:** 5 min  
**Peg Condition:**  
- When DM-IWF processes a Request message received from DRL.  
- When DM-IWF processes an Answer message received from an MD-IWF.
Note: Two messages are processed for each Diameter-to-MAP transaction: the Request received from DRL (e.g., CLR) and the Answer response received from a SS7-MP and returned to the Diameter network (e.g., CLA).

Note: This measurement serves as baseline for calculating measurements $\text{RxDmiwfDtoMTransRateAvg}$ and $\text{RxDmiwfDtoMTransRatePeak}$, as well as KPI Diameter-to-MAP Trans Msg Rate in DM-IWF KPIs.

Recovery:

No action required.

**RxDmiwfDtoMTransRateAvg**

**Measurement Group:** DM-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Avg  
**Description:** Average number of Diameter-to-MAP transaction messages processed per second.

Note: Two messages are processed for each Diameter-to-MAP transaction: the Request received from DRL (e.g., CLR) and the Answer response received from a SS7-MP and returned to the Diameter network (e.g., CLA).

**Collection Interval:** 5 min  
**Peg Condition:** Each time measurement $\text{RxDmiwfDtoMTransCnt}$ is sampled.

Recovery:

1. Determine if the Application Routing Table is mis-configured and sending too much traffic to this DSR Application. Verify the configuration from Main Menu > Diameter > Configuration > Application Routing Rules
2. Determine if there are an insufficient number of DA-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. Contact My Oracle Support (MOS) for assistance.

**RxDmiwfDtoMTransRatePeak**

**Measurement Group:** DM-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Max  
**Description:** Peak number of Diameter-to-MAP transaction messages processed per second.

Note: Two messages are processed for each Diameter-to-MAP transaction: the Request received from DRL (e.g., CLR) and the Answer response received from a SS7-MP and returned to the Diameter network (e.g., CLA).

**Collection Interval:** 5 min  
**Peg Condition:** Each time measurement $\text{RxDmiwfDtoMTransCnt}$ is sampled.

Recovery:
No action required.

**RxDmiwfMtoDTransCnt**

**Measurement Group:** DM-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** Number of MAP-to-Diameter transaction messages processed.  
**Collection Interval:** 5 min  
**Peg Condition:**  
• When DM-IWF processes a Request message received from an MD-IWF.  
• When DM-IWF processes an Answer message received from DRL.  
**Note:** Two messages are processed for each MAP-to-Diameter transaction: the Request received from a SS7-MP (e.g., CLR) and the Answer response received from DRL and returned to the SS7-MP (e.g., CLA).  
**Recovery:**  
No action required.

**RxDmiwfMtoDTransRateAvg**

**Measurement Group:** DM-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Avg  
**Description:** Average number of MAP-to-Diameter transaction messages processed per second.  
**Note:** Two messages are processed for each MAP-to-Diameter transaction: the Request received from a SS7-MP (e.g., CLR) and the Answer response received from DRL and returned to the SS7-MP (e.g., CLA).  
**Collection Interval:** 5 min  
**Peg Condition:** Each time measurement `RxDmiwfMtoDTransCnt` is sampled.  
**Recovery:**  
No action required.

**RxDmiwfMtoDTransRatePeak**

**Measurement Group:** DM-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Max  
**Description:** Peak number of MAP-to-Diameter transaction messages processed per second.
Note: Two messages are processed for each MAP-to-Diameter transaction: the Request received from a SS7-MP (e.g., CLR) and the Answer response received from DRL and returned to the SS7-MP (e.g., CLA).

**Collection Interval:** 5 min

**Peg Condition:** Each time measurement $RxDmiwfMtoDTransCnt$ is sampled.

**Recovery:**

No action required.

**$RxDmiwfTransactionRspQueuePeak$**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Max

**Description:** The peak Transaction Response Queue utilization (0-100%) measured during the collection interval. Values above 100% can be seen briefly during high traffic load conditions.

**Collection Interval:** 5 min

**Peg Condition:** The maximum Transaction Response Queue utilization sample taken during the collection interval.

**Recovery:**

No action required.

**$RxDmiwfTransactionRspQueueAvg$**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Avg

**Description:** The average Transaction Response Queue utilization (0-100%) measured during the collection interval. Values above 100% can be seen briefly during high traffic load conditions.

**Collection Interval:** 5 min

**Peg Condition:** The average of all Transaction Response Queue utilization samples taken during the collection interval.

**Recovery:**

No action required.

**$EvDmiwfPtrPoolPeak$**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Max
Measurements

**Description:** The peak DM-IWF PTR Pool utilization (0-100%) measured during the collection interval. Values above 100% can be seen briefly during high traffic load conditions.

**Collection Interval:** 5 min

**Peg Condition:** The maximum DM-IWF PTR Pool utilization sample taken during the collection interval

**Recovery:**

No action required.

**EvDmiwfPtrPoolAvg**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Avg

**Description:** The DM-IWF PTR Buffer Pool Average Utilization

**Collection Interval:** 5 min

**Peg Condition:** The average DM-IWF PTR Pool utilization sample taken during the collection interval. Values above 100% can be seen briefly during high traffic load conditions.

**Recovery:**

No action required.

**RxDmiwfRequestMessage**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Arrayed (by Command Code)

**Measurement Type:** Simple

**Description:** Number of Request messages with Command Code "X" received from DRL.

**Collection Interval:** 5 min

**Peg Condition:** Each time DM-IWF processes a Request message received from DRL.

**Recovery:**

No action required.

**RxDmiwfAnswerMessage**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Arrayed (by Command Code)

**Measurement Type:** Simple

**Description:** Number of Answer messages with Command Code "X" received from DRL.
Measurements

Collection Interval: 5 min

Peg Condition: Each time DM-IWF processes an Answer message received from DRL.

Recovery:
No action required.

**TxDmiwfRequestMessage**

- **Measurement Group**: DM-IWF Performance
- **Measurement Dimension**: Arrayed (by Command Code ID)
- **Measurement Type**: Simple
- **Description**: Number of Request messages with Command Code "X" received from DRL.
- **Collection Interval**: 5 min

Peg Condition: Each time DM-IWF successfully enqueues a Request message to DRL’s Request Queue, which includes Request messages forwarded from MD-IWFs and Request messages forwarded back to DRL for "Unavailability Action" handling.

Recovery:
No action required.

**TxDmiwfAnswerMessage**

- **Measurement Group**: DM-IWF Performance
- **Measurement Dimension**: Arrayed (by Command Code)
- **Measurement Type**: Simple
- **Description**: Number of Answer messages with Command Code "X" sent to from DRL.
- **Collection Interval**: 5 min

Peg Condition: Each time DM-IWF successfully enqueues an Answer message to DRL’s Answer Queue.

Recovery:
No action required.

**RxDmiwfRequestMessageIwf**

- **Measurement Group**: DM-IWF Performance
- **Measurement Dimension**: Single
- **Measurement Type**: Simple
- **Description**: Number of Request messages processed from am SS7-MP.
- **Collection Interval**: 5 min
Measurements

**Peg Condition:** Each time DM-IWF processes a request message received from an MD-IWF (SS7-MP).

**Recovery:**

No action required.

**RxDmiwfAnswerMessageIwf**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Description:** Number of Answer messages processed by DM-IWF that were received from an SS7-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time DM-IWF processes an Answer message received from an MD-IWF (SS7-MP).

**Recovery:**

No action required.

**TxDmiwfRequestMessageIwf**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Description:** Number of Request messages sent to an SS7-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time DM-IWF sends a Request message to an MD-IWF (SS7-MP).

**Recovery:**

No action required.

**TxDmiwfAnswerMessageIwf**

**Measurement Group:** DM-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Description:** Number of Answer messages sent to an SS7-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time DM-IWF sends a Request message to an MD-IWF (SS7-MP).

**Recovery:**

No action required.
Egress Throttle Group Performance measurements

The Diameter Egress Throttle Group Performance measurement report contains measurements providing information related to a specific ETG.

Table 54: Diameter Egress Throttle Group Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxEtgMsgsLocal</td>
<td>Number of Messages send to members of ETG. This measurement is not aggregate across all MPs but specific for this MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxEtgMsgRatePeak</td>
<td>Peak Aggregated ETG Request Message Rate calculation made during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>TxEtgMsgRateAvg</td>
<td>Average ETG Request Message Rate calculation made during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgRateCongestionOnset</td>
<td>Number of times an ETG Message Rate Congestion Level was advanced</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgRateDiscardPri0</td>
<td>Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgRateDiscardPri1</td>
<td>Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgRateDiscardPri2</td>
<td>Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgPendingTransPeak</td>
<td>Peak pending transactions to members of this ETG during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgPendingTransAvg</td>
<td>Average Pending transactions to this ETG during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgPendingTransOnset</td>
<td>Number of times an ETG Pending Transaction Limiting Congestion Level was advanced</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgPendingTransDiscardPri0</td>
<td>Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited</td>
<td>5 min</td>
</tr>
<tr>
<td>EvEtgPendingTransDiscardPri1</td>
<td>Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited</td>
<td>5 min</td>
</tr>
</tbody>
</table>
## Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvEtgPendingTransDiscardPri2</td>
<td>Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**TxEtgMsgsLocal**

**Measurement Group:** Egress Throttle Group Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by ETG ID)  
**Description:** Number of messages (Request or Answer) send on a Connection or a Peer which is part of ETG.  
**Collection Interval:** 5 min  
**Peg Condition:** When DRL successfully queues a message (Request (including Reroutes and MessageCopy) or Answer) to DCL for transmission to Connection or a Peer which is part of ETG. This peg is incremented even if ETG Rate Limiting function is Disabled. This peg is incremented only for "Routable" messages i.e messages terminated in DCL layer (eg CEX, DWX) are not counted.  
**Measurement Scope:** Site  
**Recovery:**  
   No action required

**TxEtgMsgRatePeak**

**Measurement Group:** Egress Throttle Group Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Arrayed (by ETG ID)  
**Description:** Peak Aggregated ETG Message Rate calculation made during the collection interval  
**Collection Interval:** 5 min  
**Peg Condition:** An ETG Message Rate calculation \( A_t \) is periodically calculated. If the new \( A_t \) exceeds any previous \( A_{t-k} \) value for the collection interval, then this measurement will be updated with the new \( A_t \) value.  
**Measurement Scope:** Site  
**Recovery:**  
   No action required
**TxEtgMsgRateAvg**

- **Measurement Group:** Egress Throttle Group Performance
- **Measurement Type:** Avg
- **Measurement Dimension:** Arrayed (by ETG ID)
- **Description:** Average ETG Message Rate calculation made during the collection interval
- **Collection Interval:** 5 min
- **Peg Condition:** Each time an ETG Message Rate calculation $A_i$ is calculated.
- **Measurement Scope:** Site
- **Recovery:**
  - No action required

**EvEtgRateCongestionOnset**

- **Measurement Group:** Egress Throttle Group Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by ETG ID)
- **Description:** Number of times an ETG-RCL was advanced.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time the EMR Congestion Level is advanced
- **Measurement Scope:** Site
- **Recovery:**
  1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
  2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
  3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
  4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
  5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
  6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
  7. If the problem persists, contact *My Oracle Support (MOS).*
EvEtgRateDiscardPri0

**Measurement Group:** Egress Throttle Group Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by ETG ID)  
**Description:** Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time that Routing Layer discarded a Priority 0 Request message due to last connection evaluated being ETG Rate Limited  
**Measurement Scope:** Site  
**Recovery:**  
1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.  
2. Adjust the EMR onset / abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.  
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.  
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.  
5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.  
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.  

EvEtgRateDiscardPri1

**Measurement Group:** Egress Throttle Group Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by ETG ID)  
**Description:** Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time that Routing Layer discarded a Priority 1 Request message due to last connection evaluated being ETG Rate Limited  
**Measurement Scope:** Site
Recovery:
1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
7. If the problem persists, contact My Oracle Support (MOS).

EvEtgRateDiscardPri2

Measurement Group: Egress Throttle Group Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by ETD ID)
Description: Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited.
Collection Interval: 5 min
Peg Condition: Each time that Routing Layer discarded a Priority 2 Request message due to last connection evaluated being ETG Rate Limited
Measurement Scope: Site
Recovery:
1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.

7. If the problem persists, contact *My Oracle Support (MOS).*

**EvEtgPendingTransPeak**

- **Measurement Group:** Egress Throttle Group Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Arrayed (by ETG ID)
- **Description:** Peak pending transactions to members of this ETG during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time a new $P_t$ value exceeds any previous $P_{t-k}$ value.
- **Measurement Scope:** Site
- **Recovery:** No action required

**EvEtgPendingTransAvg**

- **Measurement Group:** Egress Throttle Group Performance
- **Measurement Type:** Avg
- **Measurement Dimension:** Arrayed (by ETG ID)
- **Description:** Peak pending transactions to members of this ETG during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time a an ETG Pending Request $P_t$ value is calculated.
- **Measurement Scope:** Site
- **Recovery:** No action required

**EvEtgPendingTransCongestionOnset**

- **Measurement Group:** Egress Throttle Group Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by ETG ID)
- **Description:** Number of times an ETG-PCL was advanced.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time the ETG Window Congestion Level is advanced
Measurements

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact My Oracle Support (MOS).

EvEtgPendingTransDiscardPri0

Measurement Group: Egress Throttle Group Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by ETG ID)
Description: Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited
Collection Interval: 5 min
Peg Condition: Each time that Routing Layer discarded a Priority 0 Request message due to last connection evaluated being ETG Pending Transaction Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact *My Oracle Support (MOS)*.

**EvEtgPendingTransDiscardPri1**

**Measurement Group:** Egress Throttle Group Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by ETG ID)  
**Description:** Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited  
**Collection Interval:** 5 min  
**Peg Condition:** Each time that Routing Layer discarded a Priority 1 Request message due to last connection evaluated being ETG Pending Transaction Limited  
**Measurement Scope:** Site  

**Recovery:**

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.  
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.  
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.  
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.  
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.  
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.  
7. If the problem persists, contact *My Oracle Support (MOS)*.

**EvEtgPendingTransDiscardPri2**

**Measurement Group:** Egress Throttle Group Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by ETG ID)  
**Description:** Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited  
**Collection Interval:** 5 min  
**Peg Condition:** Each time that Routing Layer discarded a Priority 2 Request message due to last connection evaluated being ETG Pending Transaction Limited  
**Measurement Scope:** Site
Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact My Oracle Support (MOS).

Full Address Based Resolution (FABR) Application Exception measurements

The "FABR Application Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the FABR feature.

**Table 55: FABR Application Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxFabrBlacklistedImsi</td>
<td>Number of request messages received containing IMSI of a Blacklisted subscriber.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrBlacklistedMsisdn</td>
<td>Number of request messages received containing MSISDN of Blacklisted subscriber.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrDecodeFailureResol</td>
<td>Number of Request messages rejected due to a message decoding error.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrInvalidImsiMcc</td>
<td>Number of times an AVP instance present in a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailAll</td>
<td>Total number of Request messages received which did not resolve a Destination address.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxFabrResolFailCmdcode</td>
<td>Number of Request messages received with an unknown Command Code.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailImpiMatch</td>
<td>Number of Request messages received for which IMPI was used for Destination address resolution, but no Destination address was found.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailImpuMatch</td>
<td>Number of Request messages received for which IMPU was used for Destination address resolution, but no Destination address was found.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailImsiMatch</td>
<td>Number of Request messages received for which IMSI was used for Destination address resolution, but no Destination address was found.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailMsisdnMatch</td>
<td>Number of Request messages received for which MSISDN was used for Destination address resolution, but no Destination address was found.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailNoAddrAvps</td>
<td>Number of Request messages received without a Routing Entity Address AVP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolFailNoValidAddr</td>
<td>Number of Request messages received with at least Routing Entity Address AVP but no valid Routing Entity Addresses were found.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrUnkApplId</td>
<td>Number of Request messages rejected due to an unknown Application ID.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrDbConFail</td>
<td>Number of database queries failed due to the Communication Agent queue exhaustion.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrFwdFail</td>
<td>Number of routing attempt failures due to internal resource exhaustion.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
**RFabBlacklistedImsi**

- **Measurement Group:** Full Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** The number of request messages received containing IMSI of a Blacklisted subscriber
- **Collection Interval:** 5 min
- **Peg Condition:** Each time the Routing Exception “BlackListed Subscriber” is invoked
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**RFabBlacklistedMsisdn**

- **Measurement Group:** Full Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** The number of request messages received containing MSISDN of Blacklisted subscriber
- **Collection Interval:** 5 min
- **Peg Condition:** Each time the Routing Exception “BlackListed Subscriber” is invoked
- **Measurement Scope:** Server Group
- **Recovery:**
  1. Validate which User identity address is not blacklisted by using DP configuration.
  2. If the problem persists, contact My Oracle Support (MOS).

**RFabDecodeFailureResol**

- **Measurement Group:** Full Address Resolution Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of Request messages rejected due to a message decoding error.
- **Collection Interval:** 5 min
- **Peg Condition:** For each routing exception when the Application ID is not valid or the AVP extends beyond the length of the message indicated by the Message Length parameter in the message header.
- **Measurement Scope:** Server Group
- **Recovery:**
Contact My Oracle Support (MOS) for assistance.

**RxFabrInvalidImsiMcc**

**Measurement Group:** Full Address Resolution Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of times an AVP instance present in a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.  
**Collection Interval:** 5 min 
**Peg Condition:** Each time a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Validate the ranges configured in the Reserved MCC Ranges table.  
2. Verify that the MCC portion of the decodable IMSI received by RBAR does not fall within the configured Reserved MCC Ranges.  
3. If the problem persists, contact My Oracle Support (MOS).

**RxFabrResolFailAll**

**Measurement Group:** Full Address Resolution Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Total number of Request messages received which did not resolve a Destination address.  
**Collection Interval:** 5 min  
**Peg Condition:** For each Request message which did not resolve to a Destination address.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Validate which destination address is associated with the user identity address by using DP GUI.  
2. Contact My Oracle Support (MOS) for assistance.

**RxFabrResolFailCmdcode**

**Measurement Group:** Full Address Resolution Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)
Measurements

**RxFabrResolFailDpCongested**
- **Measurement Group:** Full Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Number of Database queries that failed to be serviced due DP/ComAgent errors.
- **Collection Interval:** 5 min
- **Peg Condition:** When FABR application received service notification indicating Database (DP) or DB connection (ComAgent) Errors (DP timeout, errors, or ComAgent internal errors) for the sent database query.
- **Measurement Scope:** Server Group
- **Recovery:**

**RxFabrResolFailImpiMatch**
- **Measurement Group:** Full Address Resolution Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Number of Request messages received for which IMPI was used for Destination address resolution, but no Destination address was found.
- **Collection Interval:** 5 min
- **Peg Condition:** For each message which did not successfully resolve to a Destination using a Routing Entity Type of IMPI.
- **Measurement Scope:** Server Group
- **Recovery:**
  1. Validate which destination address is associated with the user identity address by using DP GUI.
  2. Contact *My Oracle Support (MOS)* for assistance.

**Description:** Number of Request messages received with an unknown Command Code.

**Collection Interval:** 5 min

**Peg Condition:** For each routing exception where the (Application ID, Command Code) pair in the incoming Request message is not configured.

**Measurement Scope:** Server Group

**Recovery:**
- The currently provisioned Diameter Application IDs can be viewed in the FABR Configuration & Maintenance GUI.
- Contact *My Oracle Support (MOS)* for assistance.
**RxFabrResolFailImpuMatch**

**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request messages received for which IMPU was used for Destination address resolution, but no Destination address was found.  
**Collection Interval:** 5 min  
**Peg Condition:** For each message which did not successfully resolve to a Destination using a Routing Entity Type of IMPU.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Validate which destination address is associated with the user identity address by using DP GUI.  
2. Contact *My Oracle Support (MOS)* for assistance.

**RxFabrResolFailImsiMatch**

**Measurement Group:** Full Address Resolution Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request messages received for which IMSI was used for Destination address resolution, but no Destination address was found.  
**Collection Interval:** 5 min  
**Peg Condition:** For each message which did not successfully resolve to a Destination using a Routing Entity Type of IMSI.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. Validate which destination address is associated with the user identity address by using DP GUI.  
2. Contact *My Oracle Support (MOS)* for assistance.

**RxFabrResolFailMsisdnMatch**

**Measurement Group:** Full Address Resolution Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request messages received for which MSISDN was used for Destination address resolution, but no Destination address was found.  
**Collection Interval:** 5 min
**Peg Condition:** For each message which did not successfully resolve to a Destination using a Routing Entity Type of MSISDN.

**Measurement Scope:** Server Group

**Recovery:**

Validate which destination address is associated with the user identity address by using DP GUI. Contact *My Oracle Support (MOS)* for assistance.

**RxFabrResolFailNoAddrAvps**

**Measurement Group:** Full Address Resolution Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Request messages received without a Routing Entity Address AVP.

**Collection Interval:** 5 min

**Peg Condition:** For each routing exception with no valid User Identity address found and the number of AVPs searched for the message was 0.

**Measurement Scope:** Server Group

**Recovery:**

If this event is considered abnormal, then use validate which AVPs are configured for routing with the Application ID and Command Code using the FABR GUI screen. Contact *My Oracle Support (MOS)* for assistance.

**RxFabrResolFailNoValidAddr**

**Measurement Group:** Full Address Resolution Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Request messages received with at least Routing Entity Address AVP but no valid Routing Entity Addresses were found.

**Collection Interval:** 5 min

**Peg Condition:** For each routing exception with no valid User Identity address found and the number of AVPs searched for the message was greater than 0.

**Measurement Scope:** Server Group

**Recovery:**

1. If this event is considered abnormal, then use validate which AVPs are configured for routing with the Application ID and Command Code using the FABR GUI screen.
2. Contact *My Oracle Support (MOS)* for assistance.
**RxFabrSrvNotiDpComAgentErrors**

*Measurement Group:* Full Address Resolution Exception  
*Measurement Dimension:* Arrayed (per Diameter Application)  
*Measurement Type:* Simple  
*Description:* Number of failed Database queries received in the service notifications from Com Agent indicating DP/COM Agent errors.  
*Collection Interval:* 5 min  
*Peg Condition:* When FABR receives a service notification from Communication Agent indicating a DP/Communication Agent error.  
*Measurement Scope:* MP  
*Recovery:*  
  No action necessary.

**RxFabrUnkAppId**

*Measurement Group:* Full Address Resolution Performance  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* Number of Request messages rejected due to an unknown Application ID.  
*Collection Interval:* 5 min  
*Peg Condition:* For each routing exception when the Application ID is not valid.  
*Measurement Scope:* Server Group  
*Recovery:*  
  1. The currently provisioned Diameter Application IDs can be viewed in the FABR Configuration & Maintenance GUI.  
  2. The currently provisioned Application Routing Rules can be viewed using Main Menu > Diameter > Configuration > Application Routing Rules.  
  3. Contact My Oracle Support (MOS) for assistance.

**TxFabrDbConFail**

*Measurement Group:* Full Address Resolution Exception  
*Measurement Type:* Simple  
*Measurement Dimension:* Arrayed (by Diameter Application ID)  
*Description:* Number of database queries failed due to the Communication Agent queue exhaustion.  
*Collection Interval:* 5 min
Peg Condition: Each time the application attempts to send DP queries and fails due to Communication Agent queue exhaustion.

Measurement Scope: Server Group

Recovery:
Contact My Oracle Support (MOS) for assistance.

**TxFabrFwdFail**

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of routing attempt failures due to internal resource exhaustion.

Collection Interval: 5 min

Peg Condition: Each time the application attempts to enqueue a Request message on the DSR Relay Agent’s “Request Message Queue” or enqueue a Answer message on “DRL Answer Queue” and it fails (e.g., queue full).

Measurement Scope: Server Group

Recovery:
Contact My Oracle Support (MOS) for assistance.

**Full Address Based Resolution (FABR) Application Performance measurements**

The "FABR Application Performance" measurement group is a set of measurements that provide performance information that is specific to the FABR feature. These measurements will allow you to determine how many messages are successfully forwarded and received to and from the FABR Application.

**Table 56: DSR Application Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>FabrAverageQueriesPerBundle</td>
<td>Average number of queries per Bundle sent by FABR</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDpResponseTimeAvg</td>
<td>Average time (in milliseconds) it takes to receive a DP response after sending the correlated database query.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrAvgMsgSize</td>
<td>Average size of Request message received.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxFabrBundledResponseEvents</td>
<td>The number of Bundled Response Events received by FABR.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrDpResponseMsgQueueAvg</td>
<td>The average DP Response Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrDpResponseMsgQueuePeak</td>
<td>The peak DSR Application's DP Response Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrMsgs</td>
<td>Number of Request messages received by FABR application.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolAll</td>
<td>Number of Addresses Successfully Resolved to a Destination</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolAllMp</td>
<td>Number of Addresses Successfully Resolved to a Destination by the MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResollImpi</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IMPI.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResollImpu</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IMPU.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResollImsi</td>
<td>Number of Addresses Successful Resolved with Routing Entity type IMSI.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolMsisdn</td>
<td>Number of Addresses Successful Resolved with Routing Entity type MSISDN.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolRateAvg</td>
<td>Average Addresses Successfully Resolved per second</td>
<td>5 min</td>
</tr>
<tr>
<td>RxFabrResolRatePeak</td>
<td>Peak Addresses Successfully Resolved per second.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrAbandonRequest</td>
<td>Number of Request message that are abandoned.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrBundledQueryEvents</td>
<td>Number of Bundled Query Events sent to ComAgent.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxFabrFwdDefaultDest</td>
<td>Number of Request message forwarding attempts using a Default Destination.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrFwdNochange</td>
<td>Number of Request message forwarding attempts without changing the message.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrFwdSuccess</td>
<td>Number of Request messages successfully forwarded (all reasons).</td>
<td>5 min</td>
</tr>
<tr>
<td>TxFabrMsgAttempt</td>
<td>Number of Request message forwarding attempts (all reasons).</td>
<td>5 min</td>
</tr>
</tbody>
</table>

#### FabrAverageQueriesPerBundle
- **Measurement Group:** Full Address Resolution Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** Average number of queries per Bundle sent by FABR
- **Collection Interval:** 5 min
- **Peg Condition:** When FABR successfully sends a Bundled query event to ComAgent for processing
- **Measurement Scope:** Server Group
- Recovery: No action required.

#### RxDpResponseTimeAvg
- **Measurement Group:** Full Address Resolution Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** Average time (in milliseconds) it takes to receive a DP response after sending the correlated database query.
- **Collection Interval:** 5 min
- **Peg Condition:** It is calculated based on the total number of sampled database queries during the collection interval.
- **Measurement Scope:** MP
- Recovery:
No action necessary.

**RxFabrAvgMsgSize**

- **Measurement Group:** Full Address Resolution Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Arrayed (by Diameter Application ID)
- **Description:** Average size of Request message received.
- **Collection Interval:** 5 min
- **Peg Condition:** Average calculated for each Request message received.
- **Measurement Scope:** Server Group
- **Recovery:** No action necessary.

**RxFabrBundledResponseEvents**

- **Measurement Group:** Full Address Resolution Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of Bundled Response Events received by FABR.
- **Collection Interval:** 5 min
- **Peg Condition:** When FABR successfully receives a Bundled response event from ComAgent.
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**RxFabrDpResponseMsgQueueAvg**

- **Measurement Group:** Full Address Resolution Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The average DP Response Message Queue utilization (0-100%) measured during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** The average of all Request Message Queue utilization samples taken during the collection interval.
- **Measurement Scope:** Server Group
Recovery:

This alarm may occur due to persistent overload conditions with respect to database response processing.

Contact My Oracle Support (MOS) for assistance.

RxFabrDpResponseMsgQueuePeak

Measurement Group: Full Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The peak DSR Application's DP Response Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum DP Response Message Queue utilization sample taken during the collection interval.
Measurement Scope: Server Group
Recovery:

This alarm may occur due to persistent overload conditions with respect to database response processing.

Contact My Oracle Support (MOS) for assistance.

RxFabrMsgs

Measurement Group: Full Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request messages received by FABR application.
Collection Interval: 5 min
Peg Condition: For each message successfully de-queued from the application’s internal “Message Event” queue.
Measurement Scope: Server Group
Recovery:

No action necessary.

RxFabrResolAll

Measurement Group: Full Address Resolution Performance
Measurement Type: Simple
**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Addresses Successfully Resolved to a Destination.

**Collection Interval:** 5 min

**Peg Condition:** For each message successfully resolved to a Destination.

**Measurement Scope:** Server Group

**Recovery:**

No action necessary.

---

**RxFabrResolAllMp**

**Measurement Group:** Full Address Resolution Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of Addresses Successfully Resolved to a Destination by the MP.

**Collection Interval:** 5 min

**Peg Condition:** For each message successfully resolved to a Destination by the MP.

**Measurement Scope:** Server Group

**Recovery:**

No action necessary.

---

**RxFabrResolImpi**

**Measurement Group:** Full Address Resolution Performance

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Diameter Application ID)

**Description:** Number of Addresses Successful Resolved with Routing Entity type IMPI.

**Collection Interval:** 5 min

**Peg Condition:** For each message successfully resolved to a Destination using a Routing Entity Type of IMPI.

**Measurement Scope:** Server Group

**Recovery:**

No action necessary.

---

**RxFabrResolImpu**

**Measurement Group:** Full Address Resolution Performance

**Measurement Type:** Simple
**Measurement Dimension**: Arrayed (by Diameter Application ID)

**Description**: Number of Addresses Successful Resolved with Routing Entity type IMPU.

**Collection Interval**: 5 min

**Peg Condition**: For each message successfully resolved to a Destination using a Routing Entity Type of IMPU.

**Measurement Scope**: Server Group

**Recovery**: No action necessary.

---

**RxFabrResolImsi**

**Measurement Group**: Full Address Resolution Performance

**Measurement Type**: Simple

**Measurement Dimension**: Arrayed (by Diameter Application ID)

**Description**: Number of Addresses Successful Resolved with Routing Entity type IMSI.

**Collection Interval**: 5 min

**Peg Condition**: For each message successfully resolved to a Destination using a Routing Entity Type of IMSI.

**Measurement Scope**: Server Group

**Recovery**: No action necessary.

---

**RxFabrResolMsisdn**

**Measurement Group**: Full Address Resolution Performance

**Measurement Type**: Simple

**Measurement Dimension**: Arrayed (by Diameter Application ID)

**Description**: Number of Addresses Successful Resolved with Routing Entity type MSISDN.

**Collection Interval**: 5 min

**Peg Condition**: For each message successfully resolved to a Destination using a Routing Entity Type of MSISDN.

**Measurement Scope**: Server Group

**Recovery**: No action necessary.
**RxFabrResolRateAvg**

**Measurement Group:** Full Address Resolution Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** Average Addresses Successfully Resolved per second.  
**Collection Interval:** 5 min  
**Peg Condition:** The “average per second” is periodically calculated based on the total number of addresses successfully resolved.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**RxFabrResolRatePeak**

**Measurement Group:** Full Address Resolution Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** Peak Addresses Successfully Resolved per second.  
**Collection Interval:** 5 min  
**Peg Condition:** At the end of each sample period associated with average successfully resolved message rate, as defined by measurement **RxFabrResolRateAvg**, if the value exceeds the current value for this measurement, then the measurement will be updated with the current sample periods value.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.

**RxFabrSrvNotiDpCongest**

**Measurement Group:** Full Address Resolution Exception  
**Measurement Type:** Simple  
**Description:** Number of Service Notifications received from ComAgent indicating DP is congested with CL=2 or CL=3.  
**Collection Interval:** 5 min  
**Peg Condition:** When FABR receives Service Notification from ComAgent indicating a DP congestion at CL=2 or CL=3.  
**Measurement Scope:** MP
Recovery:
No action necessary.

TxFabrAbandonRequest
Measurement Group: Full Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request message that are abandoned.
Collection Interval: 5 min
Peg Condition: Each time the Routing Exception “Abandon Request” is invoked.
Measurement Scope: Server Group
Recovery:
No action necessary.

TxFabrBundledQueryEvents
Measurement Group: Full Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Bundled Query Events sent to ComAgent.
Collection Interval: 5 min
Peg Condition: When FABR successfully sends a Bundled query event to ComAgent for processing
Measurement Scope: Server Group
Recovery:
No action required.

TxFabrFwdDefaultDest
Measurement Group: Full Address Resolution Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Diameter Application ID)
Description: Number of Request message forwarding attempts using a Default Destination.
Collection Interval: 5 min
Peg Condition: Each time the Routing Exception “Forward route the message with a user-configurable Default Destination” is invoked.
Measurement Scope: Server Group
Recovery:
No action necessary.

**TxFabrFwdNochange**

**Measurement Group:** Full Address Resolution Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request message forwarding attempts without changing the message.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time the Routing Exception “Forward route the message unchanged” is invoked.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action necessary.

**TxFabrFwdSuccess**

**Measurement Group:** Full Address Resolution Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request messages successfully forwarded (all reasons).  
**Collection Interval:** 5 min  
**Peg Condition:** Each time the application successfully enqueues a Request message on the DSR Relay Agent’s Request Message Queue.  
**Measurement Scope:** Server Group  
**Recovery:**  
If this value is less than **TxFabrMsgAttempt**, then an internal resource error is occurring.  
Contact *My Oracle Support (MOS)* for assistance.

**TxFabrMsgAttempt**

**Measurement Group:** Full Address Resolution Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Diameter Application ID)  
**Description:** Number of Request message forwarding attempts (all reasons).  
**Collection Interval:** 5 min
Peg Condition: Each time the application attempts to enqueue a Request message on the DSR Relay Agent’s “Request Message Queue”.

Measurement Scope: Server Group

Recovery:
No action necessary.

GLA Exception measurements

The GLA Exception measurement group contains measurements that provide performance information that is specific to the GLA application.

Table 57: GLA Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxGlaDecodeFailures</td>
<td>Number of GLA Requests that could not be processed due to incorrect data in the Diameter message</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaDatabaseFailures</td>
<td>Number of GLA Requests that could not be processed due to pSBR-B query failure</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaDatabaseTimeouts</td>
<td>Number of GLA Requests that could not be processed due to pSBR-B query timeout</td>
<td>5 min</td>
</tr>
</tbody>
</table>

RxGlaDecodeFailures

Measurement Group: GLA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of GGRs unsuccessfully processed due to unsupported Application ID, Command Code, Subscriber Info, or other decoding issue.

Collection Interval: 5 min

Peg Condition: During GGR failure handling

Measurement Scope: Server Group

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, contact My Oracle Support (MOS).

RxGlaDatabaseFailures

Measurement Group: GLA Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of GGRs unsuccessfully processed due to queries to pSBR-B receiving a negative acknowledgment.
Collection Interval: 5 min
Peg Condition: During pSBR-B query failures
Measurement Scope: Server Group
Recovery:
1. Examine the current state of the pSBR-B via the Communication Agent > Maintenance > HA Service Status screen.
2. The status of the Reporting Server’s BindingRd should be examined to verify that all SubResources are Available. This will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, contact My Oracle Support (MOS).

RxGlaDatabaseTimeouts

Measurement Group: GLA Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of GGRs unsuccessfully processed due to queries to pSBR-B timing out before a response is received.
Collection Interval: 5 min
Peg Condition: During pSBR-B query failures
Measurement Scope: Server Group
Recovery:
1. Examine the current state of the pSBR-B via the Communication Agent > Maintenance > HA Service Status screen.
2. The status of the Reporting Server’s BindingRd should be examined to verify that all SubResources are Available. This will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, contact My Oracle Support (MOS).
GLA Performance measurements

The GLA Performance measurement group contains measurements that provide performance information that is specific to the GLA application.

Table 58: GLA Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxGlaSuccessMsgs</td>
<td>Number of GLA requests that were successfully processed</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaResponseMsgQueuePeak</td>
<td>Peak utilization of pSBR-B response queue</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaResponseMsgQueueAvg</td>
<td>Average Utilization of pSBR-B response queue</td>
<td>5 min</td>
</tr>
<tr>
<td>TxGlaSuccessMsgRatePeak</td>
<td>Peak rate of GLA Requests that are successfully processed</td>
<td>5 min</td>
</tr>
<tr>
<td>TxGlaSuccessMsgRateAvg</td>
<td>Average rate of GLA Requests that are successfully processed</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGlaFailureMsgs</td>
<td>Number of GLA requests that were not successfully processed (for any reason)</td>
<td>5 min</td>
</tr>
</tbody>
</table>

TxGlaSuccessMsgs

**Measurement Group:** GLA Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of GGRs successfully processed  
**Collection Interval:** 5 min  
**Peg Condition:** When a GGA is transmitted following a successful query of the pSBR database  
**Measurement Scope:** Server Group  
**Recovery:**  
This number can be compared against *RxGlaRequestProcessed* to get a ratio of total input Requests to successfully processed Requests.

RxGlaResponseMsgQueuePeak

**Measurement Group:** GLA Performance  
**Measurement Type:** Simple
**Measurement Dimension**: Single  
**Description**: Peak utilization of GLA’s response queue that handles pSBR-B replies.  
**Collection Interval**: 5 min  
**Peg Condition**: Reception of a response Stack Event from pSBR-B.  
**Measurement Scope**: Server Group  
**Recovery**:  
1. This number provides an indication of short-term work-rate of the response task. If this value crosses 75%, it indicates that processing rates are increasing and additional capacity may need to be added to the DSR.  
2. If the problem persists, contact *My Oracle Support (MOS)*.

**RxGlaResponseMsgQueueAvg**

**Measurement Group**: GLA Performance  
**Measurement Type**: Simple  
**Measurement Dimension**: Single  
**Description**: Average utilization of GLA’s response queue that handles pSBR-B replies.  
**Collection Interval**: 5 min  
**Peg Condition**: Reception of a response Stack Event from pSBR-B.  
**Measurement Scope**: Server Group  
**Recovery**:  
1. This number provides an indication of sustained work-rate of the response task. If this value crosses 50%, it indicates that processing rates are increasing and additional capacity may need to be added to the DSR.  
2. If the problem persists, contact *My Oracle Support (MOS)*.

**TxGlaSuccessMsgRatePeak**

**Measurement Group**: GLA Performance  
**Measurement Type**: Simple  
**Measurement Dimension**: Single  
**Description**: Peak rate of GGRs successfully processed  
**Collection Interval**: 5 min  
**Peg Condition**: When a GGA is transmitted following a successful query of the pSBR database  
**Measurement Scope**: Server Group  
**Recovery**:  
1. This number provides an indication of peak success work-rate of GLA. If can be used to determine when GLA is processing more than a customer's work-rate.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**TxGlaSuccessMsgRateAvg**

*Measurement Group:* GLA Performance  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* Average rate of GGRs successfully processed  
*Collection Interval:* 5 min  
*Peg Condition:* When a GGA is transmitted following a successful query of the pSBR database  
*Measurement Scope:* Server Group  
*Recovery:*  
1. This number provides an indication of sustained success work-rate of GLA. If can be used to determine when GLA is processing more than a customer’s work-rate.  
2. If the problem persists, contact *My Oracle Support (MOS)*.

**RxGlaFailureMsgs**

*Measurement Group:* GLA Performance  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* Number of GGRs unsuccessfully processed due to any problem.  
*Collection Interval:* 5 min  
*Peg Condition:* Any failure during processing  
*Measurement Scope:* Server Group  
*Recovery:*  
1. When non-zero, examine other failure measurements (*RxGlaDecodeFailures, RxGlaDatabaseFailures, RxGlaDatabaseTimeouts*) to isolate reasons for failures  
2. Search the Event History for additional information to identify the specific failure.  
3. If the problem persists, contact *My Oracle Support (MOS)*.

**IDIH measurements**

The IDIH measurement report contains measurements that provide performance information that is specific to the IDIH feature.
<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvIdihNumTtrsSent</td>
<td>Number of TTRs sent to DIH</td>
<td>5 min</td>
</tr>
<tr>
<td>EvIdihNumTtrsDeliveryFailed</td>
<td>Number of TTRs that could not be sent to DIH due to ComAgent connection failure</td>
<td>5 min</td>
</tr>
<tr>
<td>TmIdihTraceSuspendedTime</td>
<td>Amount of time that trace limiting is active</td>
<td>5 min</td>
</tr>
<tr>
<td>TmIdihTraceThrottlingTime</td>
<td>Amount of time that trace throttling is in force</td>
<td>5 min</td>
</tr>
<tr>
<td>EvIdihThrottlingTtrsDiscarded</td>
<td>Number of TTRs discarded due to trace throttling</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**EvIdihNumTtrsSent**

*Measurement Group:* IDIH  
*Measurement Type:* Simple  
*Description:* The number of TTRs that were sent from DSR to DIH.  
*Collection Interval:* 5 min  
*Peg Condition:* Each time a TTR is successfully transmitted from DSR to DIH.  
*Recovery:* No action required

**EvIdihNumTtrsDeliveryFailed**

*Measurement Group:* IDIH  
*Measurement Type:* Simple  
*Description:* The number of TTRs that could not be sent from DSR to DIH due to the failure of the ComAgent link.  
*Collection Interval:* 5 min  
*Peg Condition:* Each time a TTR cannot be successfully transmitted from DSR to DIH.  
*Recovery:* Re-establish the ComAgent link to DIH.

**TmIdihTraceSuspendedTime**

*Measurement Group:* IDIH  
*Measurement Type:* Duration  
*Description:* The amount of time that trace limiting is active  
*Collection Interval:* 5 min  
*Peg Condition:* Each time trace limiting is activated and stopped when trace limiting is de-activated.
Recovery:
No action required

**TmIdihTraceThrottlingTime**

Measurement Group: IDIH  
Measurement Type: Duration  
Description: The amount of time that trace throttling is active.  
Collection Interval: 5 min  
Peg Condition: Each time trace throttling is activated and stopped when trace throttling is de-activated.  
Recovery:  
No action required

**EvIdihThrottlingTtrsDiscarded**

Measurement Group: IDIH  
Measurement Type: Simple  
Description: The number of TTRs discarded due to trace throttling.  
Collection Interval: 5 min  
Peg Condition: Each time a TTR is discarded due to trace throttling.  
Recovery:  
No action required

**IP Front End (IPFE) Exception measurements**

The "IPFE Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events specific to the IPFE application. Measurements such as the following are included in this group.

**Table 59: IPFE Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PcapDroppedPackets</td>
<td>Number of ARP/ICMP/ICMPv6 control packets dropped</td>
<td>5 min</td>
</tr>
<tr>
<td>ThrottledPackets</td>
<td>Number of packets dropped due to throttling</td>
<td>5 min, 30 min, 60 min</td>
</tr>
<tr>
<td>TsaUnexpectedSctp</td>
<td>Number of SCTP packets sent to a TSA configured as “TCP Only”.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TsUnexpctedTcp</td>
<td>Number of TCP packets sent to a TSA configured as “SCTP Only”.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxReject</td>
<td>Number of new associations rejected</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRejectSctp</td>
<td>Number of new SCTP associations rejected</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**PcapDroppedPackets**

- **Measurement Group:** IPFE Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** ARP/ICMP/ICMPv6 control packets dropped. The pcap library listens for packets on the network interfaces on behalf of the IPFE. If the network interface receives more packets than it can handle, the library will drop packets and increase a dropped packet counter.
- **Collection Interval:** 5 minutes
- **Peg Condition:** This measurement is incremented by one each time the IPFE drops an ARP/ICMP/ICMPv6 control packet.
- **Measurement Scope:** Network, NE, Server Group

**Recovery:**

1. In the unlikely event that counts should appear for this measurement, network diagnostics should be performed.
2. For further assistance, contact *My Oracle Support (MOS).*

**ThrottledPackets**

- **Measurement Group:** IPFE Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of packets dropped due to throttling
- **Collection Interval:** 5 min, 30 min, 60 min
- **Peg Condition:** When a packet is dropped to limit excessive IPFE CPU
- **Measurement Scope:** Network

**Recovery:**

- Increase DSR Capacity.
Measurements

TsaUnexpectedSctp

**Measurement Group:** IPFE Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by TSA ID)

**Description:** Number of SCTP packets sent to a TSA configured as “TCP Only”.

**Collection Interval:** 5 minutes

**Peg Condition:** Incremented when an SCTP packet is received for a TSA configured as “TCP Only”.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**

Check client configuration for clients attempting SCTP associations with a TCP-only TSA.

TsaUnexpectedTcp

**Measurement Group:** IPFE Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by TSA ID)

**Description:** Number of TCP packets sent to a TSA configured as “SCTP Only”.

**Collection Interval:** 5 minutes

**Peg Condition:** Incremented when a TCP packet is received for a TSA configured as “SCTP Only”.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**

Check client configuration for clients attempting TCP connections on an SCTP-only TSA.

TxReject

**Measurement Group:** IPFE Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by TSA ID)

**Description:** Number of new associations rejected. The IPFE rejects new associations when there are no available applications servers for the target set address. The associated alarm, 5009 - No available servers in target set, will also be issued.

**Collection Interval:** 5 minutes

**Peg Condition:** This measurement is incremented by one each time the IPFE rejects a new association for a target set address.

**Measurement Scope:** Network, NE, Server Group

**Recovery:**
Check the status of the application servers by navigating to the Status & Manage > Server page.

**TxRejectSctp**

*Measurement Group:* IPFE Exception  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* New SCTP associations rejected.  
*Collection Interval:* 5 minutes  
*Peg Condition:* Incremented when an SCTP association is rejected.  
*Measurement Scope:* Network, NE, Server Group  
*Recovery:* None required

**IP Front End (IPFE) Performance measurements**

The “IPFE Performance” measurement group contains measurements that provide performance information that is specific to the IPFE application. Counts for various expected/normal messages and events are included in this group. Measurements such as the following are included.

**Table 60: IPFE Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsNewAssociations</td>
<td>Number of new associations for each server</td>
<td>5 min</td>
</tr>
<tr>
<td>AsNewAssociationsSctp</td>
<td>Number of new SCTP associations for each server</td>
<td>5 min</td>
</tr>
<tr>
<td>IpfeNewAssociations</td>
<td>Number of new associations for the IPFE</td>
<td>5 min</td>
</tr>
<tr>
<td>IpfeNewAssociationsSctp</td>
<td>Number of new SCTP associations for the IPFE</td>
<td>5 min</td>
</tr>
<tr>
<td>RxIpfeBytes</td>
<td>Number of bytes received by the IPFE</td>
<td>5 min</td>
</tr>
<tr>
<td>RxIpfeBytesSctp</td>
<td>Number of SCTP bytes received by the IPFE</td>
<td>5 min</td>
</tr>
<tr>
<td>RxIpfePackets</td>
<td>Number of packets received by the IPFE</td>
<td>5 min</td>
</tr>
<tr>
<td>RxTsaBytes</td>
<td>Number of bytes received for each TSA</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxTsaBytesSctp</td>
<td>Number of SCTP bytes received for each TSA</td>
<td>5 min</td>
</tr>
<tr>
<td>RxTsaPackets</td>
<td>Number of packets received for each TSA</td>
<td>5 min</td>
</tr>
<tr>
<td>RxTsaPacketsSctp</td>
<td>Number of SCTP packets received for each TSA</td>
<td>5 min</td>
</tr>
<tr>
<td>TsaNewAssociations</td>
<td>Number of new associations for each TSA</td>
<td>5 min</td>
</tr>
<tr>
<td>TsaNewAssociationsSctp</td>
<td>Number of new SCTP associations for each TSA</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAsBytes</td>
<td>Number of bytes sent for each server</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAsBytesSctp</td>
<td>Number of SCTP bytes sent for each server</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAsPackets</td>
<td>Number of packets sent for each server</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAsPacketsSctp</td>
<td>Number of SCTP packets sent for each server</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**AsNewAssociations**

**Measurement Group:** IPFE Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Application Server ID)  
**Description:** New associations for each server  
**Collection Interval:** 5 minutes  
**Peg Condition:** This measurement is incremented by one each time the IPFE associates a client packet with an application server.  
**Measurement Scope:** Network, NE, Server Group  
**Recovery:** None required

**AsNewAssociationsSctp**

**Measurement Group:** IPFE Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Application Server ID)  
**Description:** New SCTP associations for each server,
**Measurements**

**Collection Interval:** 5 minutes

**Peg Condition:** Incremented when a new SCTP association is established for an application server.

**Measurement Scope:** Network, NE, Server Group

**Recovery:** None required

**IpfeNewAssociations**

- **Measurement Group:** IPFE Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** New associations for the IPFE
- **Collection Interval:** 5 minutes
- **Peg Condition:** This measurement is incremented by one each time the IPFE associates a client packet with an application server.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:** None required

**IpfeNewAssociationsSctp**

- **Measurement Group:** IPFE Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** New SCTP associations for the IPFE
- **Collection Interval:** 5 minutes
- **Peg Condition:** Incremented when a new SCTP association is established through an IPFE.
- **Measurement Scope:** Network, NE, Server Group
- **Recovery:** None required

**RxIpfeBytes**

- **Measurement Group:** IPFE Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of bytes received by the IPFE.
- **Collection Interval:** 5 minutes, 30 minutes, 60 minutes
- **Peg Condition:** The measurement is incremented by one for each byte the IPFE receives.
- **Measurement Scope:** Network, NE, Server Group
Measurements

Recovery: None required

RxIpfeBytesSctp

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of SCTP bytes received by the IPFE.
Collection Interval: 5 minutes, 30 minutes, 60 minutes
Peg Condition: Incremented by the packet payload size when an SCTP packet is received by the IPFE.
Measurement Scope: Network, NE, Server Group
Recovery: None required

RxIpfePackets

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: Packets received by the IPFE
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one for each packet the IPFE receives.
Measurement Scope: Network, NE, Server Group
Recovery: None required

RxTsaBytes

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: Bytes received for each TSA.
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time a byte is received for a particular target set address.
Measurement Scope: Network, NE, Server Group
Recovery: None required
RxTsaBytesSctp

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: SCTP bytes received for each TSA.
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time an SCTP byte is received for a particular target set address.
Measurement Scope: Network, NE, Server Group
Recovery: None required

RxTsaPackets

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: Packets received for each TSA
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time a packet is received for a particular TSA.
Measurement Scope: Network, NE, Server Group
Recovery: None required

RxTsaPacketsSctp

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: SCTP packets received for each TSA.
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time an SCTP packet is received for a particular TSA.
Measurement Scope: Network, NE, Server Group
Recovery: None required
TsaNewAssociations

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: New associations for each target set address
Collection Interval:
Peg Condition: This measurement is incremented by one each time the IPFE associates a client packet with a target set address.
Measurement Scope: Network, NE, Server Group
Recovery: None required

TsaNewAssociationsSctp

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: New SCTP associations for each TSA.
Collection Interval: 5 minutes
Peg Condition: Incremented when a new SCTP association is established for a TSA.
Measurement Scope: Network, NE, Server Group
Recovery: None required

TxAsBytes

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: Bytes sent for each server
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time a byte is sent to a particular application server.
Measurement Scope: Network, NE, Server Group
Recovery: None required
TxAsBytesSctp

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by TSA ID)
Description: SCTP bytes sent for each server
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time an SCTP byte is sent to a particular application server.
Measurement Scope: Network, NE, Server Group
Recovery: None required

TxAsPackets

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Application Server ID)
Description: Packets sent for each server.
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time a packet is sent to a particular application server.
Measurement Scope: Network, NE, Server Group
Recovery: None required

TxAsPacketsSctp

Measurement Group: IPFE Performance
Measurement Type: Simple
Measurement Dimension: Arrayed (by Application Server ID)
Description: SCTP packets sent for each server.
Collection Interval: 5 minutes
Peg Condition: This measurement is incremented by one each time an SCTP packet is sent to a particular application server.
Measurement Scope: Network, NE, Server Group
Recovery: None required
MD-IWF Exception Measurements

The MD-IWF Exception measurement report contains measurements providing information about transaction processing exceptions that are specific to the MAP-Diameter IWF Application running on a SS7-MP.

Table 61: MD-IWF Exception Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxMdIwfSs7TransmitFailure</td>
<td>Number of outgoing SS7 messages to the SS7 network that could not be routed (e.g. queue full)</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfOrphanMapResponse</td>
<td>Number of orphan MAP Response messages received</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfMapResponseTimeout</td>
<td>Number of timeouts waiting for MAP Response</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfDiamNon2xxxAnswer</td>
<td>Number of Diameter Non-2xxx Answers received</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfOrphanDiamAnswer</td>
<td>Number of orphan Diameter Answer messages received</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfDiamAnswerTimeout</td>
<td>Number of timeouts waiting for Diameter Answer</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfDiamAnswerUnexpectedDaMp</td>
<td>MD-IWF received Diameter Answer from unexpected DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfFailComAgentEnqueue</td>
<td>Number of times MD-IWF failed to enqueue a Diameter message to ComAgent</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfComAgentError</td>
<td>Number of Diameter Request messages sent to DA-MP that resulted in ComAgent error / timeout or in DM-IWF NACK</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfDiamPduPoolEmpty</td>
<td>Number of messages discarded when Diameter PDU pool is exhausted</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfInterwrkFail</td>
<td>Number of interworking attempts that failed for any reason (internal or because of something from the far end)</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfInterwrkFailAddrTrans</td>
<td>Number of interworking attempts that failed while attempting Address Translation (either MAP-&gt;Diameter or Diameter-&gt;MAP)</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfInterwrkFailMsgTrans</td>
<td>Number of interworking attempts that failed while attempting message translation (encode or decode)</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TxMdIwfDiamEdlEncodeFailure</td>
<td>Number of times an EDL failure occurred while MD-IWF attempted to encode a</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>Diameter message</td>
<td></td>
</tr>
<tr>
<td>EvMdIwfInterwrkFailCongest</td>
<td>Number of interworking attempts that failed due to MD-IWF congestion</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfInterwrkFailFarEndResponse</td>
<td>Number of interworking attempts that failed due to error response received</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>from far end</td>
<td></td>
</tr>
<tr>
<td>EvMdIwfInterwrkFailDsrInitiated</td>
<td>Number of interworking attempts that failed due to action initiated by MD-IWF</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>(not due to far end)</td>
<td></td>
</tr>
<tr>
<td>EvMdIwfInterwrkFailSysError</td>
<td>Number of interworking attempts that failed due to internal processing error</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfMessageFailResExh</td>
<td>Number of times a message could not be processed due to resource exhaustion</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfTransRejectByDiamExtNode</td>
<td>Number of transactions where Diameter external node sends non-2xxx Answer</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>to DSR, and MD-IWF sends error response to SS7</td>
<td></td>
</tr>
</tbody>
</table>

**TxMdIwfSs7TransmitFailure**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** The number of outgoing SS7 messages to the SS7 network that could not be routed (e.g. queue full).  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF attempts to send a MAP message to the SS7 network (via the SS7 stack), but the message could not be routed.  
**Measurement Scope:** Site  
**Recovery:**  
Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

**RxMdIwfOrphanMapResponse**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** The number of orphan MAP Response messages received.
Collection Interval: 5 min

Peg Condition: Each time the MD-IWF Application received a MAP response message for which no Pending Transaction record exists.

Measurement Scope: Site

Recovery:
1. If this measurement is being pegged frequently, the configurable MAP Response timer may be set too low. The MAP Response Timeout value can be viewed via Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Option.
2. Contact My Oracle Support (MOS) for assistance if needed.

EvMdIwfMapResponseTimeout

Measurement Group: MD-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of timeouts waiting for MAP Response.
Collection Interval: 5 min
Peg Condition: Each time the MD-IWF Application sent a MAP request message to the SS7 network, but timed out waiting for the MAP response
Measurement Scope: Site
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 the NO GUI Main Menu > MAP-Diameter IWF > Configuration > MD-IWF Options.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxMdIwfDiamNon2xxxAnswer

Measurement Group: MD-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of Diameter Non-2xxx Answers received.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF receives a Diameter Answer message from a DA-MP where the result-Code value is non-2xxx
Measurement Scope: Site
Recovery:
Contact My Oracle Support (MOS) if this measurement is being pegged frequently.
RxMdIwfOrphanDiamAnswer

Measurement Group: MD-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of orphan Diameter Answer messages received.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF receives a Diameter Answer message for which no Pending Transaction record exists
Measurement Scope: Site
Recovery:
1. When MD-IWF sends a Diameter Request message to a DA-MP, it allocated 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. Contact My Oracle Support (MOS) for assistance if needed.

EvMdIwfDiamAnswerTimeout

Measurement Group: MD-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of timeouts following message sent to DA-MP.
Collection Interval: 5 min
Peg Condition: Each time D-IWF sends a Diameter Request message to the DA-MP, but times out waiting for the Diameter Answer
Measurement Scope: Site
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. Contact My Oracle Support (MOS) for assistance if needed.

RxMdIwfDiamAnswerUnexpectedDaMp

Measurement Group: MD-IWF Exception
Measurement Dimension: Single
**Measurement Type:** Simple

**Measurement Description:** The number of Diameter Answer messages received from unexpected DA-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time MD-IWF receives Diameter Answer from an unexpected DA-MP.

**Measurement Scope:** Site

**Recovery:**

This error is not expected to occur. Contact *My Oracle Support (MOS)* for assistance if needed.

---

**TxMdIwfFailComAgentEnqueue**

**Measurement Group:** MD-IWF Exception

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Measurement Description:** The number of times MD-IWF failed to enqueue a Diameter message to ComAgent.

**Collection Interval:** 5 min

**Peg Condition:** Each time MD-IWF attempts to send a Diameter message to a DA-MP via ComAgent, but is unable to enqueue the message.

**Measurement Scope:** Site

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

---

**RxMdIwfComAgentError**

**Measurement Group:** MD-IWF Exception

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Measurement Description:** The number of Diameter Request messages sent to DA-MP that results in ComAgent error / timeout or in DM-IWF NACK

**Collection Interval:** 5 min

**Peg Condition:** Each time MD-IWF sends a Diameter Request message to DM-IWF that results in a ComAgent error / timeout or in a DM-IWF NACK.

**Measurement Scope:** Site

**Recovery:**

No action required.
**RxMdIwfDiamPduPoolEmpty**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** The number of messages discarded when Diameter PDU pool is exhausted.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF discards a message due to Diameter PDU pool exhaustion  
**Measurement Scope:** Site  
**Recovery:**  
Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

**EvMdIwfInterwrkFail**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Measurement Description:** The total number of interworking attempts that failed for any reason (internal or because of something from the far end).  
**Collection Interval:** 5 min  
**Peg Condition:** Each time an interworking attempt by MD-IWF fails.  
**Note:** If a translation involves a Dialog Continuation and multiple messages are exchanged to perform the translation (i.e. TC-Begin, multiple TC-Continue, TC-End), then this is counted as a single interworking attempt.  
**Note:** A Diameter-initiated interworking attempt fails if the final Diameter Answer sent back has a non-2xxx result code. A MAP-initiated interworking attempt fails if the final MAP response message is an abort, error, or reject. It is also a failure if the configured Diameter Exception or MAP Exception is carried out.  
**Measurement Scope:** Site  
**Recovery:**  
Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

**EvMdIwfInterwrkFailAddrTrans**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple
**EvMdIwfInterwrkFailMsgTrans**

**Measurement Description:** The number of interworking attempts that failed while attempting message translation.

**Collection Interval:** 5 min

**Peg Condition:** Each time a failure occurs when MD-IWF attempts to perform message translation.

**Note:** Message Translation involves mapping between AVPs in a Diameter message and parameters in a MAP message.

**Measurement Scope:** Site

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

**Description:**

Number of times an EDL failure occurred while MD-IWF attempted to encode a Diameter message.

**Peg Condition:** This measurement is pegged each time MD-IWF attempts to encode a Diameter message to be sent to a DA-MP, but an EDL encode failure occurs. Event 33080 - **EDL failure occurred while MD-IWF attempted to encode a Diameter message** will be raised when this condition occurs.

**Collection Interval:** 5 min

**Measurement Scope:** Site

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.
1. If the encode failure is due to Diameter message size (failure reason can be determined from Event 33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message), it may be necessary to increase the engineering configurable parameter (DiameterMaxMessageSize in table MapIwfLongConfig) for maximum Diameter message size.

2. Contact My Oracle Support (MOS) for assistance if this measurement is being pegged frequently.

**EvMdIwfInterwrkFailCongest**
- **Measurement Group:** MD-IWF Exception
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Measurement Description:** The number of interworking attempts that failed due to MD-IWF Congestion.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time an interworking attempt by MD-IWF fails due to MD-IWF congestion.
- **Note:** If a translation involves a Dialog Continuation and multiple messages are exchanged to perform the translation (i.e. TC-BEGIN, multiple TC-CONTINUE, TC-END), then this is counted as a single interworking attempt.
- **Measurement Scope:** Site
- **Recovery:** Contact My Oracle Support (MOS) for assistance if this measurement is being pegged frequently.

**EvMdIwfInterwrkFailFarEndResponse**
- **Measurement Group:** MD-IWF Exception
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Description:** Number of interworking attempts that failed due to error response received from far end
- **Peg Condition:** This measurement is pegged each time an interworking attempt by MD-IWF fails due to receiving an error response from the far end. The error response could be a non-2xxx Diameter Answer, or a MAP U-Abort or Reject.
- **Note:** An interworking attempt is defined in *EvMdIwfInterwrkAttempt*
- **Collection Interval:** 5 min
- **Measurement Scope:** Site
- **Recovery:** Contact My Oracle Support (MOS) for assistance if this measurement is being pegged frequently.
**EvMdIwfInterwrkFailDsrInitiated**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** Number of interworking attempts that failed due to action initiated by MD-IWF (not due to far end)  
**Peg Condition:** This measurement is pegged each time an interworking attempt by MD-IWF fails due to an action initiated by MD-IWF (i.e. message translation failed, address translation failed, timeout occurred). This measurement does NOT include failures that are due to an error response received from the far end.  
**Note:** An interworking attempt is defined in *EvMdIwfInterwrkAttempt*.  
**Collection Interval:** 5 min  
**Measurement Scope:** Site  
**Recovery:**  
Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

**EvMdIwfInterwrkFailSysError**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Measurement Description:** The number of interworking attempts that failed due to internal processing error.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time an interworking attempt by MD-IWF fails due to internal processing error.  
**Note:** If a translation involves a Dialog Continuation and multiple messages are exchanged to perform the translation (i.e. TC-Begin, multiple TC-Continue, TC-End), then this is counted as a single interworking attempt.  
**Note:** Examples of internal processing errors are ComAgent error, ComAgent congestion, and resource exhaustion.  
**Measurement Scope:** Site  
**Recovery:**  
Contact *My Oracle Support (MOS)* for assistance if this measurement is being pegged frequently.

**EvMdIwfInterwrkFailResExh**

**Measurement Group:** MD-IWF Exception  
**Measurement Dimension:** Single
Measurements

Measurement Type: Simple
Measurement Description: The number of times a message could not processed due to resource exhaustion.
Collection Interval: 5 min
Peg Condition: Each time a message cannot be processed by MD-IWF due to resource exhaustion.
Note: Examples of resource exhaustion are PTR exhaustion, PDU exhaustion, and queue full.
Measurement Scope: Site
Recovery:
    Contact My Oracle Support (MOS) for assistance if this measurement is being pegged frequently.

EvMdIwfTransRejectByDiamExtNode
Measurement Group: MD-IWF Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: Number of transactions where Diameter external node sends non-2xxx Answer to DSR, and MD-IWF sends error response to SS7
Peg Condition: This measurement is pegged when a Diameter external node sends a non-2xxx Answer to DSR, which is then forwarded by DM-IWF (on DA-MP) to MD-IWF (on SS7-MP), and MD-IWF in turn sends an error response (Abort or Reject) to the SS7 network.
Collection Interval: 5 min
Measurement Scope: Site
Recovery:
    No action required

MD-IWF Performance measurements

The MD-IWF Performance measurement report contains measurements providing performance that is specific to the MAP-Diameter IWF Application running on a SS7-MP.

Table 62: MD-IWF Performance Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxMdIwfSS7Msg</td>
<td>Number of MAP messages received from the SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfSS7Msg</td>
<td>Number of MAP messages sent to SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxMdIwfMapRequestMsg</td>
<td>Number of MAP request messages received from SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfMapRequestMsg</td>
<td>Number of MAP request messages sent to SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfMapResponseMsg</td>
<td>Number of MAP response messages received from SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfMapResponseMsg</td>
<td>Number of MAP response messages sent to SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfDiamMsg</td>
<td>Number of Diameter messages received from DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfDiamMsg</td>
<td>Number of Diameter messages sent to DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfDiamRequestMsg</td>
<td>Number of Diameter Request messages received from DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfDiamAnswerMsg</td>
<td>Number of Diameter Answer messages received from DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfDiamRequestMsg</td>
<td>Number of Diameter Request messages sent to DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfDiamAnswerMsg</td>
<td>Number of Diameter Answer messages sent to DA-MP</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfInterwrkAttempt</td>
<td>Total number of interworking attempts made. One attempt includes all of the messages within a transaction that are required to perform the interworking (not counting each message). A transaction can be Diameter-originated or MAP-originated</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfInterwrkSuccess</td>
<td>Number of interworking attempts that were completely successful where the final Diameter message sent back had a result code of 2xxx or the final MAP message was a result and not an abort, error, or reject</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfIngressMsgCount</td>
<td>Total number of messages received by MD-IWF. Includes MAP msgs received from SS7 network, and Diameter msgs received from DA-MPs</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfIngressMsgRateAvg</td>
<td>Average MD-IWF ingress message rate. Includes MAP msgs received from SS7 network, and Diameter msgs received from DA-MPs</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxMdIwfIngressMsgRatePeak</td>
<td>Peak MD-IWF ingress message rate. Includes MAP msgs received from SS7 network, and Diameter msgs received from DA-MPs</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMap2DiamTransMsgCount</td>
<td>Total number of MAP-to-Diameter transaction msgs received by MD-IWF</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMap2DiamTransMsgRateAvg</td>
<td>Average MAP-to-Diameter transaction message rate</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMap2DiamTransMsgRatePeak</td>
<td>Peak MAP-to-Diameter transaction message rate</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiam2MapTransMsgCount</td>
<td>Total number of Diameter-to-MAP transaction msgs received by MD-IWF</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiam2MapTransMsgRateAvg</td>
<td>Average Diameter-to-MAP transaction message rate</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiam2MapTransMsgRatePeak</td>
<td>Peak Diameter-to-MAP transaction message rate</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiMdwfDiamTransMsgQueuePeak</td>
<td>Peak DiamTrans Task Message Queue utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiMdwfDiamTransMsgQueueAvg</td>
<td>Average DiamTrans Task Message Queue utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiMdwfMapTransMsgQueuePeak</td>
<td>Peak MapTrans Task Message Queue utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiMdwfMapTransMsgQueueAvg</td>
<td>Average MapTrans Task Message Queue utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiMdwfDampInterfaceMsgQueuePeak</td>
<td>Peak DampInterface Task Message Queue utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxDiMdwfDampInterfaceMsgQueueAvg</td>
<td>Average DampInterface Task Message Queue utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfDiam2MapPtrUtilPeak</td>
<td>Peak DiamToMap PTR utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfDiam2MapPtrUtilAvg</td>
<td>Average DiamToMap PTR utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfMap2DiamPtrUtilPeak</td>
<td>Peak MapToDiam PTR utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMdIwfMap2DiamPtrUtilAvg</td>
<td>Average MapToDiam PTR utilization</td>
<td>5 min</td>
</tr>
<tr>
<td>TmMdIwfMap2DiamPtrTotalHoldTimeAvg</td>
<td>Average hold time (in milliseconds) of MAP-to-Diameter transactions processed by MD-IWF</td>
<td>5 min</td>
</tr>
<tr>
<td>TmMdIwfDiam2MapPtrTotalHoldTimeAvg</td>
<td>Average hold time (in milliseconds) of Diameter-to-MAP transactions processed by MD-IWF</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvMdIwfTransSuccessByDiamExtNode</td>
<td>Number of transactions where Diameter external node sends success (2xxx) Answer to DSR, and MD-IWF sends success response to SS7</td>
<td>5 min</td>
</tr>
</tbody>
</table>

#### RxMdIwfSS7Msg

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Description:** The number of MAP messages received from the SS7 network.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time MD-IWF receives a MAP message from the SS7 network. This includes both request and response messages.
- **Measurement Scope:** Site
- **Recovery:**  
  - No action required.

#### TxMdIwfSS7Msg

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Description:** The number of MAP messages sent to SS7 network.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time MD-IWF sends a MAP message to the SS7 network. This includes both request and response messages.
- **Measurement Scope:** Site
- **Recovery:**  
  - No action required.

#### RxMdIwfMapRequestMsg

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
Measurements

**TxMdIwfMapRequestMsg**
- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Description:** The number of MAP request messages to SS7 network.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time MD-IWF sends a MAP request message to the SS7 network.
- **Measurement Scope:** Site
- **Recovery:** No action required.

**RxMdIwfMapResponseMsg**
- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Description:** The number of MAP response messages received from SS7 network.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time MD-IWF receives a MAP response message from the SS7 network.
- **Measurement Scope:** Site
- **Recovery:** No action required.

**TxMdIwfMapResponseMsg**
- **Measurement Group:** MD-IWF Performance
- **Measurement Type:** Simple
- **Description:** The number of MAP response messages sent to SS7 network.
Measurements

Collection Interval: 5 min

Peg Condition: Each time MD-IWF sends a MAP response message to the SS7 network. This measurement counts "success" responses, but doesn’t count errors, rejects, or aborts.

Measurement Scope: Site

Recovery:
No action required.

RxMdIwfDiamMsg

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of Diameter messages from DA-MP.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF receives a Diameter message from a DA-MP. This includes both Request and Answer messages.
Measurement Scope: Site
Recovery:
No action required.

TxMdIwfDiamMsg

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of Diameter successfully sent to DA-MP.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF sends a Diameter message to a DA-MP. This includes both Request and Answer messages.
Measurement Scope: Site
Recovery:
No action required.

RxMdIwfDiamRequestMsg

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
**Measurement Type:** Simple  
**Description:** The number of Diameter Request messages received from DA-MP.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF receives a Diameter Request message from a DA-MP.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**RxMdIwfDiamAnswerMsg**  
**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** The number of Diameter Answer messages received from DA-MP.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF receives a Diameter Answer message from a DA-MP.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**TxMdIwfDiamRequestMsg**  
**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Simple  
**Description:** The number of Diameter Request messages sent to DA-MP.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF sends a Diameter Request message to a DA-MP  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**TxMdIwfDiamAnswerMsg**  
**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Single
**EvMdIwfInterwrkAttempt**

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Measurement Description:** Total number of interworking attempts made. One attempt includes all of the messages within a transaction that are required to perform the interworking (not counting each message). A transaction can be Diameter-originated or MAP-originated
- **Collection Interval:** 5 min
- **Peg Condition:** Each time MD-IWF attempts to translate a MAP message into a Diameter message or translate a Diameter message into a MAP message.
- **Note:** If a translation involves a Dialog Continuation and multiple messages are exchanged to perform the translation (i.e. TC-Begin, multiple TC-Continue, TC-End), then this is counted as a single interworking attempt.
- **Measurement Scope:** Site
- **Recovery:** No action required.

**EvMdIwfInterwrkSuccess**

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Simple
- **Measurement Description:** The total number of interworking attempts that were completely successful where the final Diameter message sent back had a result code of 2xxx of the final MAP message was a result and not an abort, error, or reject.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time MD-IWF successfully completes an interworking attempt.
- **Note:** If a translation involves a Dialog Continuation and multiple messages are exchanged to perform the translation (i.e. TC-Begin, multiple TC-Continue, TC-End), then this is counted as a single interworking attempt.
Note: A Diameter-initiated interworking attempt is successful if the final Diameter Answer sent back has a result code of 2xxx. A MAP-initiated interworking attempt is successful if the final MAP response message is a result and not an abort, error, or reject.

Measurement Scope: Site

Recovery:
No action required.

RxMdIwfIngressMsgCount

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Simple
Measurement Description: The total number of messages received by MD-IWF, including MAP messages received from the SS7 network and Diameter messages received from DA-MPs.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF receives a message. This number includes MAP messages that are received from the SS7 network and Diameter messages that are received from DA-MPs.

Note: This measurement serves as a baseline for calculating measurements RxMdIwfIngressMsgRateAvg and RxMdIwfIngressMsgRatePeak as well as KPI MD-IWF KPIs.

Measurement Scope: Site
Recovery:
No action required.

RxMdIwfIngressMsgRateAvg

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Average
Description: The average MD-IWF ingress message rate, including MAP messages received from SS7 network and Diameter messages received from DA-MPs.
Collection Interval: 5 min
Peg Condition: Each time KPI MD-IWF KPIs samples RxMdIwfIngressMsgCount.

Measurement Scope: Site
Recovery:
No action required.

RxMdIwfIngressMsgRatePeak

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Max
Description: The peak MD-IWF ingress message rate, including MAP messages received from SS7 network and Diameter messages received from DA-MPs.
Collection Interval: 5 min
Peg Condition: Each time KPI MD-IWF KPIs samples RxMdlwflngressMsgCount.
Measurement Scope: Site
Recovery: No action required.

RxMap2DiamTransMsgCount
Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Simple
Description: The total number of MAP-to-Diameter transaction messages by MD-IWF.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF receives a MAP request message from the SS7 network and each subsequent message that MD-IWF receives in the MAP-to-Diameter transaction.
Note: For example, MD-IWF could receive a CancelLocationArg from the SS7 network, send a Diameter CLR to a DA-MP, receive a Diameter CLA from a DA-MP, and send a CancelLocationRes to the SS7 network. In this example, there are 2 messages that are pegged in the MAP-to-Diameter transaction.
Note: This measurement serves as a baseline for calculating measurements RxMap2DiamTransMsgRateAvg and RxMap2DiamTransMsgRatePeak as well as KPI MAP-to-Diameter Ingress Msg Rate found in MD-IWF KPIs.
Measurement Scope: Site
Recovery: No action required.

RxMap2DiamTransMsgRateAvg
Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Average
Description: The average MAP-to-Diameter transaction messages rate.
Collection Interval: 5 min
Peg Condition: Each time KPI MD-IWF KPIs samples RxMap2DiamTransMsgCount.
Measurement Scope: Site
Measurements

Recovery:
No action required.

RxMap2DiamTransMsgRatePeak

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Max
Description: The peak MAP-to-Diameter transaction messages rate.
Collection Interval: 5 min
Peg Condition: Each time KPI MD-IWF KPIs samples RxMap2DiamTransMsgCount.
Measurement Scope: Site
Recovery:
No action required.

RxDiam2MapTransMsgCount

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
Measurement Type: Simple
Description: The total number of Diameter-to-MAP transaction messages received by MD-IWF.
Collection Interval: 5 min
Peg Condition: Each time MD-IWF receives a Diameter Request message from a DA-MP and each subsequent message that MD-IWF receives in the Diameter-to-MAP transaction.
Note: For example, MD-IWF could receive a Diameter CLR message from the a DA-MP, send a CancelLocationArg to the SS7 Network, receive a CancelLocationRes from the SS7 network, and send a Diameter CLA to the DA-MP. In this example, there are 2 messages that are pegged in the MAP-to-Diameter transaction.
Note: This measurement serves as a baseline for calculating measurements RxDiam2MapTransMsgRateAvg and RxDiam2MapTransMsgRatePeak as well as KPI MD-IWF KPIs.
Measurement Scope: Site
Recovery:
No action required.

RxDiam2MapTransMsgRateAvg

Measurement Group: MD-IWF Performance
Measurement Dimension: Single
**Measurement**

**Measurement Type:** Average  
**Description:** The average Diameter-to-MAP transaction message rate.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time KPI *MD-IWF KPIs* samples *RxDiam2MapTransMsgCount*.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**RxDiam2MapTransMsgRatePeak**  
**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Single  
**Measurement Type:** Max  
**Description:** The peak Diameter-to-MAP transaction message rate.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time KPI *MD-IWF KPIs* samples *RxDiam2MapTransMsgCount*.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**RxMdIwfDiamTransMsgQueuePeak**  
**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Arrayed (by Task ID)  
**Measurement Type:** Max  
**Description:** The peak DiamTrans Task Message Queue utilization.  
**Collection Interval:** 5 min  
**Peg Condition:** For each DiamTrans task, this peg represents the maximum DiamTrans Task Message Queue utilization sample taken during the collection interval.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**RxMdIwfDiamTransMsgQueueAvg**  
**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Arrayed (by Task ID)
**RxMdIwfMapTransMsgQueuePeak**

**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Arrayed (by Task ID)  
**Measurement Type:** Max  
**Description:** The peak MapTrans Task Message Queue utilization.  
**Collection Interval:** 5 min  
**Peg Condition:** For each MapTrans task, this peg represents the maximum MapTrans Task Message Queue utilization sample taken during the collection interval.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**RxMdIwfMapTransMsgQueueAvg**

**Measurement Group:** MD-IWF Performance  
**Measurement Dimension:** Arrayed (by Task ID)  
**Measurement Type:** Average  
**Description:** The average MapTrans Task Message Queue utilization.  
**Collection Interval:** 5 min  
**Peg Condition:** For each MapTrans task, this peg represents the average MapTrans Task Message Queue utilization sample taken during the collection interval.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.
**RxMdIwfDampInterfaceMsgQueuePeak**

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Max
- **Description:** The peak DampInterface Task Message Queue utilization.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg represents the maximum DAMPInterface Task Message Queue utilization sample taken during the collection interval.
- **Measurement Scope:** Site
- **Recovery:**
  - No action required.

**RxMdIwfDampInterfaceMsgQueueAvg**

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Average
- **Description:** The average DampInterface Task Message Queue utilization.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg represents the average DAMPInterface Task Message Queue utilization sample taken during the collection interval.
- **Measurement Scope:** Site
- **Recovery:**
  - No action required.

**EvMdIwfDiam2MapPtrUtilPeak**

- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Max
- **Description:** The peak DiamToMap PTR utilization.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg represents the maximum DiamToMap PTR utilization sample taken during the collection interval.
- **Measurement Scope:** Site
- **Recovery:**
No action required.

**EvMdIwfDiam2MapPtrUtilAvg**
- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Average
- **Description:** The average DiamToMap PTR utilization.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg represents the average DiamToMap PTR utilization sample taken during the collection interval.
- **Measurement Scope:** Site
- **Recovery:**
  - No action required

**EvMdIwfMap2DiamPtrUtilPeak**
- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Max
- **Description:** The peak MapToDiam PTR utilization.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg represents the maximum MapToDiam PTR utilization sample taken during the collection interval.
- **Measurement Scope:** Site
- **Recovery:**
  - No action required

**EvMdIwfMap2DiamPtrUtilAvg**
- **Measurement Group:** MD-IWF Performance
- **Measurement Dimension:** Single
- **Measurement Type:** Average
- **Description:** The average MapToDiam PTR utilization.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg represents the average MapToDiam PTR utilization sample taken during the collection interval.
**Measurement Scope:** Site

**Recovery:**

No action required

---

**TmMdIwfMap2DiamPtrTotalHoldTimeAvg**

**Measurement Group:** MD-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Average

**Description:** Average hold time (in milliseconds) of MAP-to-Diameter transactions processed by MD-IWF

**Peg Condition:** The transaction hold time begins when a MAP-to-Diam Pending Transaction Record (PTR) is allocated and ends when the PTR is deallocated. This measurement is pegged when the PTR is deallocated.

**Measurement Scope:** Site

**Recovery:**

No action required

---

**TmMdIwfDiam2MapPtrTotalHoldTimeAvg**

**Measurement Group:** MD-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Average

**Description:** Average hold time (in milliseconds) of Diameter-to-MAP transactions processed by MD-IWF

**Peg Condition:** The transaction hold time begins when a Diam-to-MAP Pending Transaction Record (PTR) is allocated and ends when the PTR is deallocated. This measurement is pegged when the PTR is deallocated.

**Measurement Scope:** Site

**Recovery:**

No action required

---

**EvMdIwfTransSuccessByDiamExtNode**

**Measurement Group:** MD-IWF Performance

**Measurement Dimension:** Single

**Measurement Type:** Simple

**Description:** Number of transactions where Diameter external node sends success (2xxx) Answer to DSR, and MD-IWF sends success response to SS7
Peg Condition: This measurement is pegged when a Diameter external node sends a success (2xxx) Answer to DSR, which is then forwarded by DM-IWF (on DA-MP) to MD-IWF (on SS7-MP), and MD-IWF in turn sends a success response (not an Abort or Reject) to the SS7 network.

Measurement Scope: Site

Recovery:
No action required

MD-IWF SS7 Performance measurements

The MD-IWF SS7 Performance measurement report contains measurements providing performance that is specific to the MAP-Diameter IWF Application running on a SS7-MP.

Table 63: MD-IWF SS7 Performance Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxMdIwfMapRequestMsgByOpcode</td>
<td>Number of MAP request messages with Op Code &quot;X&quot; received from SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfMapResponseMsgByOpcode</td>
<td>Number of MAP response messages with Op Code &quot;X&quot; received from SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfMapRequestMsgByOpcode</td>
<td>Number of MAP request messages with Op Code &quot;X&quot; sent to SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfMapResponseMsgByOpcode</td>
<td>Number of MAP response messages with Op Code &quot;X&quot; sent to SS7 network</td>
<td>5 min</td>
</tr>
</tbody>
</table>

RxMdIwfMapRequestMsgByOpcode

Measurement Group: MD-IWF SS7 Performance

Measurement Dimension: Arrayed (by MAP Op Code)

Measurement Type: Simple

Measurement Description: The number of MAP request messages with Op Code "X" received from SS7 network.

Collection Interval: 5 min

Peg Condition: Each time MD-IWF receives a MAP request message from the SS7 network

Measurement Scope: Site

Recovery:
No action required.
**RxMdIwfMapResponseMsgByOpcode**

**Measurement Group:** MD-IWF SS7 Performance  
**Measurement Dimension:** Arrayed (by MAP Op Code)  
**Measurement Type:** Simple  
**Measurement Description:** The number of MAP response messages with Op Code "X" received from SS7 network.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF receives a MAP response message from the SS7 network.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**TxMdIwfMapRequestMsgByOpcode**

**Measurement Group:** MD-IWF SS7 Performance  
**Measurement Dimension:** Arrayed (by MAP Op Code)  
**Measurement Type:** Simple  
**Measurement Description:** The number of MAP request messages with Op Code "X" sent to SS7 network.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF sends a MAP request message to the SS7 network.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**TxMdIwfMapResponseMsgByOpcode**

**Measurement Group:** MD-IWF SS7 Performance  
**Measurement Dimension:** Arrayed (by MAP Op Code)  
**Measurement Type:** Simple  
**Measurement Description:** The number of MAP response messages with Op Code "X" sent to SS7 network.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF sends a MAP response message to the SS7 network.  
**Measurement Scope:** Site  
**Recovery:**
No action required.

MD-IWF Diam Performance Measurements

The MD-IWF Diam Performance measurement report contains measurements providing performance that is specific to the MAP-Diameter IWF Application running on a SS7-MP.

Table 64: MD-IWF Diam Performance Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxMdIwfMapRequestMsgByOpcode</td>
<td>Number of MAP request messages with Op Code &quot;X&quot; received from SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMdIwfMapResponseMsgByOpcode</td>
<td>Number of MAP response messages with Op Code &quot;X&quot; received from SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfMapRequestMsgByOpcode</td>
<td>Number of MAP request messages with Op Code &quot;X&quot; sent to SS7 network</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMdIwfMapResponseMsgByOpcode</td>
<td>Number of MAP response messages with Op Code &quot;X&quot; sent to SS7 network</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxMdIwfDiamRequestMsgByCommandCode**

**Measurement Group:** MD-IWF Diam Performance  
**Measurement Dimension:** Arrayed (by Diameter Command Code ID)  
**Measurement Type:** Simple  
**Measurement Description:** The number of Diameter Request messages with Command Code "X" received from DA-MP.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MD-IWF receives a Diameter Request message from a DA-MP.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.

**RxMdIwfDiamAnswerMsgByCommandCode**

**Measurement Group:** MD-IWF Diam Performance  
**Measurement Dimension:** Arrayed (by Diameter Command Code ID)  
**Measurement Type:** Simple
Measurements

**Measurement Description:** The number of Diameter Request messages with Command Code "X" received from DA-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time MD-IWF receives a Diameter Request message from a DA-MP.

**Measurement Scope:** Site

**Recovery:**

No action required.

**TxMdIwfDiamRequestMsgByCommandCode**

**Measurement Group:** MD-IWF Diam Performance

**Measurement Dimension:** Arrayed (by Diameter Command Code ID)

**Measurement Type:** Simple

**Measurement Description:** The number of Diameter Request messages with Command Code "X" sent to DA-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time MD-IWF sends a Diameter Request message to a DA-MP.

**Measurement Scope:** Site

**Recovery:**

No action required.

**TxMdIwfDiamAnswerMsgByCommandCode**

**Measurement Group:** MD-IWF Diam Performance

**Measurement Dimension:** Arrayed (by Diameter Command Code ID)

**Measurement Type:** Simple

**Measurement Description:** The number of Diameter Answer messages with Command Code "X" sent to DA-MP.

**Collection Interval:** 5 min

**Peg Condition:** Each time MD-IWF sends a Diameter Answer message to a DA-MP.

**Measurement Scope:** Site

**Recovery:**

No action required.
Message Copy measurements

The Diameter Application Server (DAS) measurements reflect the Message Copy performance. These measurements allow the user to monitor the amount of traffic being copied and the percentage of times that messages were successfully (or unsuccessfully) copied. Measurements such as the following are included in this group:

- Number of messages being copied
- Number of errors in transmitting those copies (i.e., retransmits)
- Number of times a copy transaction failed
- Tx and Message Copy queue utilization

Table 65: Message Copy Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASCopyAnswerRx</td>
<td>Total number of DAS Copy Answers received.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyDiscarded</td>
<td>Total number of Message Copy failures because of any error (no Answer received, the result code in the Answer didn’t match provisioning).</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyFailureMCCSNotProvisioned</td>
<td>Total amount of DAS Copy failures due to the copied message not finding a provisioned MCCS.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyFailureMPCong</td>
<td>Total number of DAS Copy Failures because the MP was congested.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyFailurePeerAppIdUnsup</td>
<td>Total amount of DAS Copy Failures because the Diameter Application Layer has specified a route list with no peer for the application ID in the message.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyFailureRLNotProv</td>
<td>Total number of DAS Copy Failures because the route list is not provisioned.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyFailureSizeExceeded</td>
<td>Total amount of DAS Copy failures due to the copied message size configured for the system.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyRetransmits</td>
<td>Total number of DAS Copy retransmits.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyRetransmitsExceeded</td>
<td>Total number of times the DAS Copy retransmits exceeded the configured max number of retransmits.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>DASCopyTx</td>
<td>Total number of DAS Copies forwarded.</td>
<td>5 min</td>
</tr>
<tr>
<td>DASCopyValidAnswer</td>
<td>Total number of DAS Copy transactions completed (a Copy Pending Transaction has been paired with a qualified Answer from the DAS peer).</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgCopyQueueAve</td>
<td>Average Message Copy Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgCopyQueueFullDiscard</td>
<td>Total number of DAS Request messages discarded because the Message Copy queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgCopyQueuePeak</td>
<td>Peak Message Copy Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**DASCopyAnswerRx**

**Measurement Group:** DAS  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The total number of DAS Copy Answers received.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an Answer response is received from a DAS peer.  
**Measurement Scope:** Server Group  
**Recovery:**  
No action required.  
This measurement is an indication of the Message Copy response traffic load being processed by the MP.

**DASCopyDiscarded**

**Measurement Group:** DAS  
**Measurement Type:** Simple  
**Measurement Dimension:** Single
Measurements

**Description:** Total number of Message Copy failures because of any error (no Answer received, the result code in the Answer didn’t match provisioning).

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a DAS Copy fails for any reason. Some failure reasons include (but are not limited to): no answer from peer, Application ID not supported at the peer, result code in the Answer incorrect/doesn’t match provisioning.

**Measurement Scope:** Server Group

**Recovery:**
1. Verify proper routing to the intended DAS peer is configured and in service (route list is properly configured), Diameter application is selecting intended route list.
2. Verify intended DAS peer is properly configured to receive the intended traffic and traffic load.
3. Verify no network issues exist between the MP and intended DAS peer.

**DASCopyFailureMCCSNotProvisioned**

**Measurement Group:** DAS

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Total amount of DAS Copy failures due to the copied message not finding a provisioned MCCS.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Copy Pending Transaction is discarded because the original message does not contain a valid MCCS, thus causing the copy action to fail.

**Measurement Scope:** Server Group

**Recovery:**
1. Verify the MCCS configured with the trigger points and ensure proper provisioning.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**DASCopyFailureMPCong**

**Measurement Group:** DAS

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Total number of DAS Copy Failures because the MP was congested.

**Collection Interval:** 5 min

**Peg Condition:** When the MP declares congestion (declared CL1-CL3), the Message Copy function is disabled. Original messages marked for copy and held as a Pending Transactions are not copied and
increment this measurement. If the Copy has been sent to the DAS peer, the Copy transaction will be allowed to complete. If the Copy transaction fails, another measurement will be incremented.

Either the MP is receiving traffic in excess of its rated capacity or the intended DAS peer is not responding in a timely fashion.

**Measurement Scope:** Server Group

**Recovery:**

1. Reduce traffic being received by the MP.
2. Verify there are no network issues between the MP and the intended DAS peer.
3. Ensure the intended DAS peer has sufficient capacity to process the traffic being directed to it by the MP

**DASCopyFailurePeerApplIdUnsup**

**Measurement Group:** DAS

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Total amount of DAS Copy Failures because the Diameter Application Layer has specified a route list with no peer for the application ID in the message.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Copy Pending Transaction is discarded because a Diameter Request has been marked for copy by the application, but no connection in the provided Route List supports the Application ID in the request, causing the copy action to fail.

**Measurement Scope:** Server Group

**Recovery:**

1. Verify the route list provisioning points to the intended DAS peer, and the intended DAS peer is responding with the desired Application ID.
2. Contact *My Oracle Support (MOS)* for assistance.

**DASCopyFailureSizeExceeded**

**Measurement Group:** DAS

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Total amount of DAS Copy failures due to the copied message size exceeding the maximum message size configured for the system.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Copy Pending Transaction is discarded because a the message being copied to the DAS exceeded the system set maximum message size, thus causing the copy action to fail.
Measurement Scope: Server Group
Recovery:
1. Verify the maximum message size set system wide is sufficient for handling the messages being processed.
2. Contact My Oracle Support (MOS) for assistance.

DASCopyFailureRLNotProv

Measurement Group: DAS
Measurement Type: Simple
Measurement Dimension: Single
Description: Total number of DAS Copy Failures because the route list is not provisioned.
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Copy Pending Transaction fails because the indicated route list contained in the Diameter request does not match what has been provisioned as a system option or other provisioned route lists.

Measurement Scope: Server Group
Recovery:
1. Review local provisioning that connections to intended DAS peer server(s) are in service and that no network issues exist in the path(s) to intended DAS peer server(s).
2. Review DAS peer provisioning to insure proper configuration.
3. Contact My Oracle Support (MOS) for assistance.

DASCopyRetransmits

Measurement Group: DAS
Measurement Type: Simple
Measurement Dimension: Single
Description: Total number of DAS Copy retransmits.
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time any Copied Message is retransmitted to a DAS peer because a qualified Diameter Answer response has not been received within the Pending Answer Timer’s timeout value to complete the pending transaction.

Measurement Scope: Server Group
Recovery:
1. Verify proper routing to the intended DAS peer is configured and in service (route list is properly configured), Diameter application is selecting intended route list.
2. Verify intended DAS peer is properly configured to receive the intended traffic and traffic load.
3. Verify no network issues exist between the MP and intended DAS peer.

**DASCopyRetransmitsExceeded**
- **Measurement Group**: DAS
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: Total number of times the DAS Copy retransmits exceeded the configured max number of retransmits.
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented each time a Copy Pending Transaction is discarded because the Copied Request has been retransmitted the configured number of times without receiving an Answer response from the DAS peer.
- **Measurement Scope**: Server Group
- **Recovery**:
  1. Verify proper routing to the intended DAS peer is configured and in service (route list is properly configured), Diameter application is selecting intended route list.
  2. Verify intended DAS peer is properly configured to receive the intended traffic and traffic load.
  3. Verify no network issues exist between the MP and intended DAS peer.

**DASCopyTx**
- **Measurement Group**: DAS
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: The total number of DAS Copies forwarded.
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented each time a Message Copy is transmitted to a DAS peer.
- **Measurement Scope**: Server Group
- **Recovery**:
  No action required.
  This measurement is an indication of the Message Copy traffic load being processed by the MP.

**DASCopyValidAnswer**
- **Measurement Group**: DAS
Measurements

Measurement Type: Simple
Measurement Dimension: Single
Description: The total number of DAS Copy transactions completed (a Copy Pending Transaction has been paired with a qualified Answer from the DAS peer).
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a Copy Pending Transaction is completed because a Diameter Copy Pending Transaction has been paired with a qualified Answer received from a DAS peer, completing the transaction.
Measurement Scope: Server Group
Recovery:
1. Verify proper routing to the intended DAS peer is selected and in service.
2. desired answer result code is provisioned in the Diameter > System Options.
3. desired DAS peer is configured to return the answer result code provisioned in the Diameter > System Options.
4. Contact My Oracle Support (MOS) for assistance.

TxMsgCopyQueueAve
Measurement Group: DAS
Measurement Type: Average
Description: The average Message Copy Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: This measurement is pegged when a new Message Copy SysMetric sample is collected, then divided by the number of samples collected in the collection period.
Measurement Scope: Server Group
Recovery:
No action required.
This is an diagnostic indicator of the amount of traffic load being processed by the Message Copy feature.

TxMsgCopyQueueFullDiscard
Measurement Group: DAS
Measurement Type: Simple
Measurement Dimension: Single
Description: Total number of DAS Request messages discarded because the Message Copy queue was full.
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a DAS Request is discarded because the Message Copy Tx queue was full, thus preventing a new DAS Request from being queued for transmit.

Measurement Scope: Server Group

Recovery:
No action required.

This is an diagnostic indicator of the amount of traffic load being processed by the Message Copy feature.

TxMsgCopyQueuePeak

Measurement Group: DAS
Measurement Type: Max
Measurement Dimension: Single
Description: The peak Message Copy Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min

Peg Condition: This measurement is pegged when a new Message Copy SysMetric sample is collected and the sample exceeds the previously saved peak for the collection period. When a new collection period is begun, the peak is reset to 0.

Measurement Scope: Server Group

Recovery:
No action required.

This is an diagnostic indicator of the amount of traffic load being processed by the Message Copy feature.

Message Priority measurements

The Message Priority measurement group contains measurements that provide information on message priority assigned to ingress Diameter messages. Measurements such as these are included in this group.

- Totals for the number of Request messages set to priority “X” when received from a peer.
- Totals for the number of Request messages set to priority “X” as a result of PRT processing.

Table 66: Message Priority Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvConnPeerUnsuppMp</td>
<td>The number of times an ingress Request was received on a connection configured to read</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TxConnUnexpMp</td>
<td>The number of times an ingress message was received with a priority of ‘3’, when the peer supports UCMP feature.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri0ApplRule</td>
<td>Number of Request messages set to priority ‘0’ as a result of ART processing</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri0Ingress</td>
<td>Total number of ingress messages assigned message priority 0.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri0PeerRule</td>
<td>Number of Request messages set to priority ‘0’ as a result of PRT processing.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri1ApplRule</td>
<td>Number of Request messages set to priority ‘1’ as a result of ART processing</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri1Ingress</td>
<td>Total number of ingress messages assigned message priority 1.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri1PeerRule</td>
<td>Number of Request messages set to priority ‘1’ as a result of PRT processing.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri2ApplRule</td>
<td>Number of Request messages set to priority ‘2’ as a result of ART processing</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri2Ingress</td>
<td>Total number of ingress messages assigned message priority 2.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgPri2PeerRule</td>
<td>Number of Request messages set to priority ‘2’ as a result of PRT processing.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**ExConnPeerUnsuppMp**

**Measurement Group:** Message Priority
**ExConnUnexpMp**

**Measurement Group:** Message Priority  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of times an ingress Request message was received with a priority of “3”, when the peer supports UCMP feature.

**Collection Interval:** 5 min  
**Peg Condition:** Pegged when a peer supports UCMP feature and an ingress Request message was received with a priority of “3”.

**Measurement Scope:** Server Group  
**Recovery:**

1. Verify that the peer is a DSR  
   - Product-Name is reported as “Eagle XG DSR”, in the Event Additional Information.  
   - Vendor-Id is reported as 323 (Tekelec).
2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.

- Call My Oracle Support (MOS) and obtain the minimum DSR software version that supports Message Priority and compare with this information.
- If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call My Oracle Support (MOS).
- If the reported Firmware-Version is less than the minimum required DSR software version, call My Oracle Support (MOS) to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to “None”.

RxMsgPri0ApplRule

Measurement Group: Message Priority
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Request messages set to priority "0" as a result of ART processing
Collection Interval: 5 min
Peg Condition: Each time DRL selects an application routing rule for routing a Request message, the rule action is set to "Route to Application", and a Message Priority of "0" is assigned to the application routing rule
Measurement Scope: Server Group
Recovery:
   No action required.

RxMpMsgPri0

Measurement Group: Message Priority
Measurement Type: Simple
Measurement Dimension: Single
Description: Total number of ingress messages assigned message priority 0.
Collection Interval: 5 min
Peg Condition: Pegged when an ingress message is assigned a priority of 0.
Measurement Scope: Server Group
Recovery:
   No action necessary.
RxMsgPri0PeerRule

**Measurement Group:** Message Priority  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of Request messages set to priority “0” as a result of PRT processing.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to “Route to Peer”, and a Message Priority of “0” is assigned to the peer routing rule.  
**Measurement Scope:** Server Group  
**Recovery:**  

No action necessary.

RxMsgPri1ApplRule

**Measurement Group:** Message Priority  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Number of Request messages set to priority “1” as a result of ART processing  
**Collection Interval:** 5 min  
**Peg Condition:** Each time DRL selects an application routing rule for routing a Request message, the rule action is set to "Route to Application", and a Message Priority of "1" is assigned to the application routing rule  
**Measurement Scope:** Server Group  
**Recovery:**  

No action required.

RxMpMsgPri1

**Measurement Group:** Message Priority  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Total number of ingress messages assigned message priority 1.  
**Collection Interval:** 5 min  
**Peg Condition:** Pegged when an ingress message is assigned a priority of 1.  
**Measurement Scope:** Server Group  
**Recovery:**
No action necessary.

**RxMsgPri1PeerRule**

- **Measurement Group:** Message Priority
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of Request messages set to priority “1” as a result of PRT processing.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to “Route to Peer”, and a Message Priority of “1” is assigned to the peer routing rule.
- **Measurement Scope:** Server Group
- **Recovery:** No action necessary.

**RxMsgPri2ApplRule**

- **Measurement Group:** Message Priority
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of Request messages set to priority “2” as a result of ART processing.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time DRL selects an application routing rule for routing a Request message, the rule action is set to “Route to Application”, and a Message Priority of “2” is assigned to the application routing rule.
- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**RxMpMsgPri2**

- **Measurement Group:** Message Priority
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Total number of ingress messages assigned message priority 2.
- **Collection Interval:** 5 min
- **Peg Condition:** Pegged when an ingress message is assigned a priority of 2.
**Measurement Scope:** Server Group
**Recovery:**
No action necessary.

**RxMsgPri2PeerRule**

**Measurement Group:** Message Priority
**Measurement Type:** Simple
**Measurement Dimension:** Single
**Description:** Number of Request messages set to priority “2” as a result of PRT processing.
**Collection Interval:** 5 min
**Peg Condition:** Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to “Route to Peer”, and a Message Priority of “2” is assigned to the peer routing rule.

**Measurement Scope:** Server Group
**Recovery:**
No action necessary.

**Message Processor (MP) Performance measurements**

The MP Performance measurement report contains measurements that provide performance information for an MP server.

**Table 67: MP Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvDiameterProcessAvg</td>
<td>The average Diameter process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvDiameterProcessPeak</td>
<td>The peak Diameter process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvLongTimeoutPtrPoolAvg</td>
<td>The average Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>EvLongTimeoutPtrPoolPeak</td>
<td>The peak Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMpCongestionEntered</td>
<td>Number of times that the MP became congested (regardless of severity level).</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMpCongestionLevel1Entered</td>
<td>The number of times that the local DA-MP entered CPU congestion level 1.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMpCongestionLevel2Entered</td>
<td>The number of times that the local DA-MP entered CPU congestion level 2.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMpCongestionLevel3Entered</td>
<td>The number of times that the local DA-MP entered CPU congestion level 3.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMpDangerOfCongestionEntered</td>
<td>The number of times that the local DA-MP entered danger of CPU congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPduPoolAvg</td>
<td>The average Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPduPoolPeak</td>
<td>The peak Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPtrPoolAvg</td>
<td>The average Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvPtrPoolPeak</td>
<td>The peak Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvStasisModeMaxConnections</td>
<td>The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to the maximum number of connections on the DA-MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvStasisModeMpCongestion</td>
<td>The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to MP Congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxAnswerMsgQueueAvg</td>
<td>The average Answer Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAnswerMsgQueuePeak</td>
<td>The peak Answer Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgRateAvgMp</td>
<td>The average MP ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero application ID).</td>
<td>5 min</td>
</tr>
<tr>
<td>RxMsgRatePeakMp</td>
<td>The peak Ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero application ID).</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRequestMsgQueueAvg</td>
<td>The average Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRequestMsgQueuePeak</td>
<td>The peak Request Message Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmAnswerTimeAvg</td>
<td>Average time (in microseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmAnswerTimePeak</td>
<td>Peak time (in microseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmMpCongestion</td>
<td>Total time (in milliseconds) spent in local MP congestion state.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmMpCongestionLevel1</td>
<td>The total time (in seconds) the local DA-MP was in CPU congestion level.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TmMpCongestionLevel2</td>
<td>The total time (in seconds) the local DA-MP was in CPU congestion level 2. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmMpCongestionLevel3</td>
<td>The total time (in seconds) the local DA-MP was in CPU congestion level 3. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmMpDangerOfCongestion</td>
<td>The total time (in milliseconds) the local DA-MP was in danger of CPU congestion. This will appear as an aggregate value retrieved from all DA-MPs for OAM Network Element.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmRequestTimeAvg</td>
<td>Average time (in microseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmRequestTimePeak</td>
<td>Peak time (in microseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAllConnQueueAvg</td>
<td>The average All-Connections Event Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAllConnQueuePeak</td>
<td>The peak All-Connections Event Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteQueueAvg</td>
<td>The average Reroute Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRerouteQueuePeak</td>
<td>The peak Reroute Queue utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
EvDiameterProcessAvg

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average Diameter Process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.

Collection Interval: 5 min

Peg Condition: The average of all Diameter process CPU utilization samples taken during the collection interval.

Measurement Scope: Server Group

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

EvDiameterProcessPeak

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak Diameter process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.

Collection Interval: 5 min

Peg Condition: The maximum Diameter process CPU utilization sample taken during the collection interval.

Measurement Scope: Server Group

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.
**EvLongTimeoutPtrPoolAvg**

**Measurement Group:** MP Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** The average Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all Diameter Long Timeout PTR Buffer Pool utilization samples taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP, then a Diameter problem may exist that is causing excessive Long Timeout traffic to be delivered to the MP. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).  
3. If the problem persists, contact *My Oracle Support (MOS)*.

**EvLongTimeoutPtrPoolPeak**

**Measurement Group:** MP Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** The peak Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.  
**A Long Timeout PTR is allocated for each Request message with a Pending Answer Timer value greater than 10 seconds that is forwarded to an upstream peer and is de-allocated when an Answer response is received and routed to a downstream peer. This measurement is useful for evaluating whether excessive traffic levels are being assigned to the Long Timeout pool. Assignment of traffic to this pool should be limited to Requests that are expected to have long response times.**  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum Diameter Long Timeout PTR Buffer Pool utilization sample taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP, then a Diameter problem may exist that is causing excessive Long Timeout traffic to be delivered to the MP. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).  
3. If the problem persists, contact *My Oracle Support (MOS)*.
problem may exist that is causing excessive Long Timeout traffic to be delivered to the MP. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

3. If the problem persists, contact *My Oracle Support (MOS)*.

**EvMpCongestionEntered**

- **Measurement Group**: MP Performance
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: The number of times that the MP became congested (regardless of severity level).
- **Collection Interval**: 5 min
- **Peg Condition**: Each time Alarm 22200 - *Local MP Congestion* transitions from cleared to asserted with severity CL1.
- **Measurement Scope**: Server Group

**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)*.

**EvMpCongestionLevel1Entered**

- **Measurement Group**: MP Performance
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: The number of times that the local DA-MP entered CPU congestion level 1.
- **Collection Interval**: 5 min
- **Peg Condition**: Each time Alarm 22200 - *Local MP Congestion* transitions from "cleared" or asserted with severity "Info" to asserted with severity "Minor".
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. DA-MP server status can be monitored from Main Menu > Status & Manage > Server Status.

2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored from Main Menu > Status & Manage > KPIs. Each DA-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 DA-MP can be monitored 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.

4. The Diameter Process may be experiencing problems. The alarm log be examined from Main Menu > Status & Manage > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

**EvMpCongestionLevel2Entered**

- **Measurement Group:** MP Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of times that the local DA-MP entered CPU congestion level 2.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time Alarm 22200 - Local MP Congestion transitions from "cleared" or asserted with severity "Info" or "Minor" to asserted with severity "Major".

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. DA-MP server status can be monitored from Main Menu > Status & Manage > Server Status.

2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored from Main Menu > Status & Manage > KPIs. Each DA-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 DA-MP can be monitored 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.

4. The Diameter Process may be experiencing problems. The alarm log be examined from Main Menu > Status & Manage > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

**EvMpCongestionLevel3Entered**

- **Measurement Group:** MP Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of times that the local DA-MP entered CPU congestion level 3.
EvMpDangerOfCongestionEntered

Measurement Group: MP Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of times that the local DA-MP entered danger of CPU congestion.
Collection Interval: 5 min
Peg Condition: Each time Alarm 22200 - Local MP Congestion transitions from "cleared" to asserted with severity “Info”.

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.
4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Status & Manage > Alarms & Events.
5. If the problem persists, contact My Oracle Support (MOS).
EvPduPoolAvg

**Measurement Group:** MP Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Single  
**Description:** The average Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all Diameter PDU Buffer Pool utilization samples taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the ingress message rate and/or Diameter process CPU utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).  
3. Contact *My Oracle Support (MOS)* for assistance if needed.

EvPduPoolPeak

**Measurement Group:** MP Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** The peak Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.  
A PDU is allocated to each message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general, PDU buffers are engineered to match the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal Diameter queues.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum Diameter PDU Buffer Pool utilization sample taken during the collection interval.  
**Measurement Scope:** Server Group  
**Recovery:**
1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the ingress message rate and/or Diameter process CPU utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

3. Contact My Oracle Support (MOS) for assistance if needed.

**EvPtrListAvg**

- **Measurement Group:** MP Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** The average Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** The average of all Diameter PTR Buffer Pool utilization samples taken during the collection interval.
- **Measurement Scope:** Server Group

**EvPtrListPeak**

- **Measurement Group:** MP Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.

A PTR is allocated for each Request message that is forwarded to an upstream peer and is de-allocated when an Answer response is received and routed to a downstream peer. This measurement is useful for evaluating whether persistent network or upstream server problems exist. In general, PTR buffers
are engineered to match the processing capacity of the MP. If network or upstream server problems exist, delaying pending transactions in the MP, then PTRs (and associated messages/PDUs) will sit in internal Diameter queues.

**Collection Interval:** 5 min

**Peg Condition:** The maximum Diameter PTR Buffer Pool utilization sample taken during the collection interval.

**Measurement Scope:** Server Group

**Recovery:**

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the ingress message rate and/or Diameter process CPU utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

3. Contact *My Oracle Support (MOS)* for assistance if needed.

**EvStasisModeMaxConnsExceeded**

**Measurement Group:** MP Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to maximum number of connections on the DA-MP.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented when the A DA-MP is sending IPFE a “heartbeat” message and it has determined that the number of Diameter connections established has reached the maximum number supported by the DA-MP since the last “heartbeat” message was sent. A DA-MP will send a “heartbeat” message indicating a STASIS availability status when it has reached its maximum number of active Diameter connections.

**Measurement Scope:** Server Group

**Recovery:**

1. If the DA-MP is a member of a IPFE TS, verify that the IPFE is configured to fully monitor the DA-MP’s availability status.

   When a IPFE fully monitors application servers in a IPFE TS, it will cease from distributing new Diameter connections to any/all application servers that report a “Stasis” availability status.

2. If the problem persists, contact *My Oracle Support (MOS).*
EvStasisModeMpCongestion

Measurement Group: MP Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The DA-MP is in MP Congestion due to high traffic rates. The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to MP Congestion.
Collection Interval: 5 min
Peg Condition: This measurement is incremented when the A DA-MP is sending IPFE a “heartbeat” message and it has been determined that its Congestion Level has transitions from CL0 (No Congestion) since the last heartbeat message sent. A DA-MP will send a “heartbeat” message indicating STASIS availability status when it’s Congestion Level is greater than CL0.
Measurement Scope: Server Group
Recovery:
1. The traffic rate needs to be decreased.
2. Contact My Oracle Support (MOS) for assistance.

RxAnswerMsgQueueAvg

Measurement Group: MP Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average Answer Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The average of all Answer Message Queue utilization samples taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxAnswerMsgQueuePeak

Measurement Group: MP Performance
Measurements

Measurement Type: Max
Measurement Dimension: Single
Description: The peak Answer Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum Answer Message Queue utilization sample taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxMsgRateAvgMp
Measurement Group: MP Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average MP ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).
Collection Interval: 5 min
Peg Condition: The average of all MP ingress message rate samples taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxMsgRatePeakMp
Measurement Group: MP Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).
Collection Interval: 5 min
Peg Condition: The maximum ingress message rate (messages per second) sample taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxRequestMsgQueueAvg
Measurement Group: MP Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average Request Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The average of all Request Message Queue utilization samples taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

RxRequestMsgQueuePeak
Measurement Group: MP Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak Request Message Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum Request Message Queue utilization sample taken during the collection interval.
Measurement Scope: Server Group
Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

TmAnswerTimeAvg
Measurement Group: MP Performance
Measurement Type: Average
Measurement Dimension: Single
Description: Average time (in milliseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.
Note: This is the average cross-MP delay for answers during the measurement period excluding ethernet/IP stack ingress and egress processing time.
Collection Interval: 5 min
Peg Condition: Timing started when an ingress Answer message is read from the connection socket. Timing stopped when the matching egress Answer message is written to the connection socket. The difference between the two times is used to update the average.
Measurement Scope: Server Group
Recovery:
1. If this measurement indicates an excessive average cross-MP delay, examine the DIAM KPIs to determine if the system is under excessive load.
2. Examine the Peer Routing Rules to determine if there are an excessive number of rules.
3. Contact My Oracle Support (MOS) for assistance if needed.
**TmAnswerTimePeak**

**Measurement Group:** MP Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** Peak time (in milliseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.  
**Note:** This is the peak cross-MP delay for answers during the measurement period excluding ethernet/IP stack ingress and egress processing time.  
**Collection Interval:** 5 min  
**Peg Condition:** Timing started when an ingress Answer message is read from the connection socket. Timing stopped when the matching egress Answer message is written to the connection socket. This measurement is pegged if the difference is larger than the current value of the measurement.  
**Measurement Scope:** Server Group  
**Recovery:** No action required.

**TmMpCongestion**

**Measurement Group:** MP Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Total time (in milliseconds) spent in local MP congestion state.  
**Collection Interval:** 5 min  
**Peg Condition:** The time duration interval starts when one of the following conditions occurs:  
1. A new collection interval for the measurement begins and alarm **22200 - Local MP Congestion** is asserted (regardless of severity level).  
2. Alarm **22200 - Local MP Congestion** is asserted with severity Minor (local MP congestion level CL0 to CL1 transition).  
The time duration interval stops when one of the following conditions occurs:  
1. The collection interval for the measurement ends and alarm **22200 - Local MP Congestion** is asserted (regardless of severity level).  
2. Alarm **22200 - Local MP Congestion** is cleared (local MP congestion level CL1 to CL0 transition).  
When a time duration interval completes, the time measured is added to the total measurement value.  
**Measurement Scope:** Server Group  
**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).

**TmMpCongestionLevel1**

**Measurement Group:** MP Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The total time (in seconds) the local DA-MP was in CPU congestion level 1. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.  
**Collection Interval:** 5 min  
**Peg Condition:**  
The "time interval" starts when one of the following conditions occur:  
• A new "collection interval" for the measurement begins and Alarm 22200 - Local MP Congestion is already asserted with severity "Minor".  
• Alarm 22200 - Local MP Congestion is asserted with severity "Minor" (onset of local DA-MP CPU congestion level 1 or abatement of local DA-MP CPU congestion levels 2 or 3).

The "time interval" stops when one of the following conditions occur:  
• The "collection interval" for the measurement ends and Alarm 22200 - Local MP Congestion is already asserted with severity "Minor".  
• Alarm 22200 - Local MP Congestion is no longer asserted with severity "Minor" (abatement of local DA-MP CPU congestion level 1 or onset of local DA-MP CPU congestion levels 2 or 3).

When the "time interval" completes, the time measured is added to the measurement value.

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. DA-MP server status can be monitored from Main Menu > Status & Manage > Server Status.

2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored from Main Menu > Status & Manage > KPIs. Each DA-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 DA-MP can be monitored 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.

4. The Diameter Process may be experiencing problems. The alarm log be examined from Main Menu > Status & Manage > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).

TmMpCongestionLevel2

Measurement Group: MP Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The total time (in seconds) the local DA-MP was in CPU congestion level 2. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.
Collection Interval: 5 min
Peg Condition:
The "time interval" starts when one of the following conditions occur:
• A new "collection interval" for the measurement begins and Alarm 22200 - Local MP Congestion is already asserted with severity "Major".
• Alarm 22200 - Local MP Congestion is asserted with severity "Major" (onset of local DA-MP CPU congestion level 2 or abatement of local DA-MP CPU congestion levels 3).
The "time interval" stops when one of the following conditions occur:
• The "collection interval" for the measurement ends and Alarm 22200 - Local MP Congestion is already asserted with severity "Major".
• Alarm 22200 - Local MP Congestion is no longer asserted with severity "Major" (abatement of local DA-MP CPU congestion level 2 or onset of local DA-MP CPU congestion levels 3).

When the "time interval" completes, the time measured is added to the measurement value.

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. DA-MP server status can be monitored from Main Menu > Status & Manage > Server Status.

2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored from Main Menu > Status & Manage > KPIs. Each DA-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 DA-MP can be monitored 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.

4. The Diameter Process may be experiencing problems. The alarm log be examined from Main Menu > Status & Manage > Alarms & Events.

5. If the problem persists, contact My Oracle Support (MOS).
TmMpCongestionLevel3

**Measurement Group:** MP Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  

**Description:** The total time (in seconds) the local DA-MP was in CPU congestion level 3. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.  

**Collection Interval:** 5 min  

**Peg Condition:**  
The "time interval" starts when one of the following conditions occur:  
- A new "collection interval" for the measurement begins and Alarm 22200 - Local MP Congestion is already asserted with severity "Critical".  
- Alarm 22200 - Local MP Congestion is asserted with severity "Critical" (onset of local DA-MP CPU congestion level 3).  

The "time interval" stops when one of the following conditions occur:  
- The "collection interval" for the measurement ends and Alarm 22200 - Local MP Congestion is already asserted with severity "Critical".  
- Alarm 22200 - Local MP Congestion is no longer asserted with severity "Critical" (abatement of local DA-MP CPU congestion level 3).  

When the "time interval" completes, the time measured is added to the measurement value.  

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. DA-MP server status can be monitored from Main Menu > Status & Manage > Server Status.  
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored from Main Menu > Status & Manage > KPIs. Each DA-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 DA-MP can be monitored 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.  
4. The Diameter Process may be experiencing problems. The alarm log be examined from Main Menu > Status & Manage > Alarms & Events.  
5. If the problem persists, contact My Oracle Support (MOS).

TmMpDangerOfCongestion

**Measurement Group:** MP Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  

**Description:** The total time (in milliseconds) the local DA-MP was in danger of CPU congestion. This value will appear as an aggregate value retrieved from all DA-MPs for OAM Network Element.
Collection Interval: 5 min

Peg Condition:

The “time interval” starts when one of the following conditions occurs:

- A new “collection interval” for the measurement begins and Alarm 22200 - Local MP Congestion is already asserted with severity “Info”.
- Alarm 22200 - Local MP Congestion is asserted with severity “Info” (onset of local DA-MP danger of CPU congestion).

The “time interval” stops when one of the following conditions occurs:

- The “collection interval” for the measurement ends and Alarm 22200 - Local MP Congestion is already asserted with severity “Info”.
- Alarm 22200 - Local MP Congestion is cleared (abatement of local DA-MP danger of CPU congestion).

When the “time interval” completes, the time measured is added to the measurement value.

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 DA-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 DA-MP from Main Menu > Status & Manage > KPIs. Each DA-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. Monitor the ingress traffic rate of each DA-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.
4. The Diameter Process may be experiencing problems. Examine the alarm log from Main Menu > Alarms & Events.
5. If the problem persists, contact My Oracle Support (MOS).

TmRequestTimeAvg

Measurement Group: MP Performance
Measurement Type: Average
Measurement Dimension: Single

Description: Average time (in milliseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.

Note: This is the average cross-MP delay for Requests during the measurement period excluding ethernet/IP stack ingress and egress processing time.

Collection Interval: 5 min

Peg Condition: Timing started when an ingress message is read from the connection socket. Timing stopped when the matching egress message is written to the connection socket. The difference between the two times is used to update the average.

Measurement Scope: Server Group
Recovery:
1. If this measurement indicates an excessive average cross-MP delay, examine the DIAM KPIs to determine if the system is under excessive load.
2. Examine the Peer Routing Rules to determine if there are an excessive number of rules.
3. Contact My Oracle Support (MOS) for assistance if needed.

TmRequestTimePeak
Measurement Group: MP Performance
Measurement Type: Max
Measurement Dimension: Single
Description: Peak time (in milliseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer’s SCTP/TCP socket until it is sent to the egress peer’s SCTP/TCP socket.
Note: This is the peak cross-MP delay for Requests during the measurement period excluding ethernet/IP stack ingress and egress processing time.
Collection Interval: 5 min
Peg Condition: Timing started when an ingress request message is read from the connection socket. Timing stopped when the matching egress request message is written to the connection socket. This measurement is pegged if the difference is larger than the current value of the measurement.
Measurement Scope: Server Group
Recovery:
   No action required.

TxAllConnQueueAvg
Measurement Group: MP Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average All-Connections Event Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The average of all All-Connections Event Queue utilization samples taken during the collection interval.
Measurement Scope: Server Group
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 DSR may be experiencing a problem preventing it from processing events from its All-Connections Event Queue. The alarm log should be examined using the Alarms & Events page.

5. If the problem persists, contact My Oracle Support (MOS).

TxAllConnQueuePeak

Measurement Group: MP Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The peak All-Connections Event Queue utilization (0-100%) measured during the collection interval.
Collection Interval: 5 min
Peg Condition: The maximum of all All-Connections Event Queue utilization samples taken during the collection interval.
Measurement Scope: Server Group
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 DSR may be experiencing a problem preventing it from processing events from its All-Connections Event Queue. The alarm log should be examined using the Alarms & Events page.

5. If the problem persists, contact My Oracle Support (MOS).

TxRerouteQueueAvg

Measurement Group: MP Performance
Measurement Type: Average
**Measurement Dimension:** Single  
**Description:** The average Reroute Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all Reroute Queue utilization samples taken during the collection interval.  
**Measurement Scope:** Server Group  

**Recovery:**  
1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer timeouts. The status of connections should be examined from the Diameter > Maintenance > Connections page.  
2. If no additional congestion alarms are asserted, the routing answer 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, contact My Oracle Support (MOS).

**TxCrerouteQueuePeak**  
**Measurement Group:** MP Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Single  
**Description:** The peak Reroute Queue utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum Reroute Queue utilization sample taken during the collection interval.  
**Measurement Scope:** Server Group  

**Recovery:**  
1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer timeouts. The status of connections should be examined from the Diameter > Maintenance > Connections page.  
2. If no additional congestion alarms are asserted, the routing answer 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, contact My Oracle Support (MOS).

**OAM.ALARM measurements**  

**Table 68: OAM Alarm measurements**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm.Crit</td>
<td>The number of critical alarms.</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

E53474 Revision 01, July 2014  

744
### OAM.PERF Measurements

#### Table 69: OAM Performance Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>appworks guiReqAvg</td>
<td>Average AppWorks GUI request time</td>
<td>5 min</td>
</tr>
<tr>
<td>appworks guiReqMax</td>
<td>Max AppWorks GUI request time</td>
<td>5 min</td>
</tr>
<tr>
<td>appworks guiReqCount</td>
<td>Number of times a particular AppWorks GUI request was made</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer awSoapInAvg</td>
<td>Average soap request server processing time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer awSoapInMax</td>
<td>Max soap request server processing time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer awSoapInCount</td>
<td>Number of times a soap request was processed</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer cmSoapOutAvg</td>
<td>Average soap request client wait time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer cmSoapOutMax</td>
<td>Max soap request client wait time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer cmSoapOutCount</td>
<td>Number of times a soap request was made</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer tpdSoapOutAvg</td>
<td>Average soap request client wait time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer tpdSoapOutMax</td>
<td>Max soap request client wait time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer tpdSoapOutCount</td>
<td>Number of times a soap request was made</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer cacheHit</td>
<td>Number of times the request cache was hit</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer cacheMiss</td>
<td>Number of times the request cache was missed</td>
<td>5 min</td>
</tr>
</tbody>
</table>

Measurements
<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>apwSoapServer.cacheClear</td>
<td>Number of times the request cache was cleared</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.auditSkip</td>
<td>Number of times an audit cycle was skipped</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.soapClient</td>
<td>Number of times a new soap client was created</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.procStart</td>
<td>Number of times the process was started</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.procSig</td>
<td>Number of times the process was signalled</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.soapReqEnQ</td>
<td>Number of soap requests enqueued</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.soapReqAvg</td>
<td>Average soap request processing time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.soapReqCount</td>
<td>Number of soap requests processed</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.soapReqMax</td>
<td>Maximum time to process a soap request (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.auditAvg</td>
<td>Average audit processing time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.auditCount</td>
<td>Number of audits processed</td>
<td>5 min</td>
</tr>
<tr>
<td>apwSoapServer.auditMax</td>
<td>Maximum time to process an audit (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>appworks.totalGuiReqAvg</td>
<td>Average GUI request processing time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>appworks.totalGuiReqMax</td>
<td>Max GUI request processing time (ms)</td>
<td>5 min</td>
</tr>
<tr>
<td>appworks.totalGuiReqCount</td>
<td>Number of GUI requests processed</td>
<td>5 min</td>
</tr>
</tbody>
</table>

### OAM.SYSTEM measurements

**Table 70: OAM System measurements**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>System.CPU_UtilPct_Average</td>
<td>The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy).</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.CPU_UtilPct_Peak</td>
<td>The peak CPU usage from 0 to 100% (100% indicates that all cores are completely busy).</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>System.Disk_UtilPct_Average</td>
<td>The average disk usage for the partition on which the COMCOL database resides.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.Disk_UtilPct_Peak</td>
<td>The peak disk usage for the partition on which the COMCOL database resides.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.RAM_UtilPct_Average</td>
<td>The average committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.RAM_UtilPct_Peak</td>
<td>The peak committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.ShMem_UtilPct_Average</td>
<td>The average shared memory usage as a percentage of the limit configured by shl.set.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.ShMem_UtilPct_Peak</td>
<td>The peak shared memory usage as a percentage of the limit configured by shl.set.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapIn_Rate_Average</td>
<td>The average number of memory pages swapped in to memory from disk per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapIn_Rate_Peak</td>
<td>The peak number of memory pages swapped in to memory from disk per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapOut_Rate_Average</td>
<td>The average number of memory pages swapped out of memory from disk per second.</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>
P-DRA Diameter Usage measurements

The P-DRA Diameter Usage measurement report contains measurements that provide performance information that is specific to the P-DRA Diameter protocol.

Table 71: P-DRA Diameter Usage Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PdraGxTopoHidingApplied</td>
<td>Number of messages received on Gx interface on which topology hiding has</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>been applied by P-DRA.</td>
<td></td>
</tr>
<tr>
<td>PdraGxpTopoHidingApplied</td>
<td>Number of Gx-Prime CC Request messages on which topology hiding is applied.</td>
<td>5 min</td>
</tr>
<tr>
<td>PdraRxTopoHidingApplied</td>
<td>Number of messages received on Rx interface on which topology hiding has</td>
<td>5 min</td>
</tr>
<tr>
<td></td>
<td>been applied by P-DRA.</td>
<td></td>
</tr>
<tr>
<td>RxBindCapApn2PcrfPool</td>
<td>Number of times a given APN is successfully mapped to a PCRF Pool</td>
<td>5 min</td>
</tr>
<tr>
<td>RxBindCap2PcrfSubPool</td>
<td>Number of binding capable session initiation requests that were mapped to a</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>PCRF Sub-Pool by a given PCRF Sub-Pool Selection Rule</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RxBindCapPcrfPool2Prt</td>
<td>Number of binding capable session initiation requests that are routed using a PRT table chosen as a result of PCRF Pool or PCRF Sub-Pool mapping to the PRT.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCcrInitNoImsiMsgs</td>
<td>Number of CCR Initial messages received without IMSI.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdra5002FromPcrf</td>
<td>Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a PCRF</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdra5002FromPolicyClient</td>
<td>Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a policy client.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraAarMsgs</td>
<td>Number of AAR messages received by PDRA.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraAsrMsgs</td>
<td>Number of ASR messages received by PDRA.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraCcrInitMsgs</td>
<td>Number of CCR Initial messages received by PDRA.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraCcrTerminateMsgs</td>
<td>Number of CCR Termination messages received by PDRA.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraCcrUpdateMsgs</td>
<td>Number of CCR Update messages received by PDRA.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraGxpBindingSuccess</td>
<td>Number of Gx-Prime CCR Initial messages processed by PDRA against binding key priorities</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraGxpCcrInitMsgs</td>
<td>Number of Gx-Prime CCR Initial messages processed by PDRA</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraGxpCcrUpdateMsgs</td>
<td>Number of Gx-Prime CCR Update messages received by PDRA</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraGxpCcrTerminateMsgs</td>
<td>Number of Gx-Prime CCR Termination messages received by PDRA</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraMsgRateAvg</td>
<td>Average Diameter ingress message processing rate of P-DRA during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraMsgRatePeak</td>
<td>Peak Diameter ingress message processing rate of P-DRA during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxPdraRarGxMsgs</td>
<td>Number of RAR messages received by PDRA for Gx interface.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraRarRxMsgs</td>
<td>Number of RAR messages received by PDRA for Rx interface.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraStrMsgs</td>
<td>Number of STR messages received by PDRA.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPdraGxRarQuery</td>
<td>Number of Gx RAR requests initiated by P-DRA for the purposes of querying for session existence at the policy client.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPdraGxRarRelease</td>
<td>Number of Gx RAR requests initiated by P-DRA for the purposes of releasing a session as a result of an error in the P-DRA.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**PdraGxTopoHidingApplied**

*Measurement Group:* P-DRA Diameter Usage  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* Number of messages received on Gx interface on which topology hiding has been applied by P-DRA.  
*Collection Interval:* 5 min  
*Peg Condition:* The measurement shall be incremented each time topology hiding is applied when a message from Gx interface is processed by the application.  
*Measurement Scope:* All  
*Recovery:* No action necessary.

**PdraGxpTopoHidingApplied**

*Measurement Group:* P-DRA Diameter Usage  
*Measurement Type:* Simple  
*Measurement Dimension:* Single  
*Description:* Number of Gx-Prime CC Request messages on which topology hiding is applied.  
*Collection Interval:* 5 min  
*Peg Condition:* Each time a Gx-Prime CC request message is processed by the P-DRA application and topology hiding is applied on the message.  
*Measurement Scope:* All
Recovery:
No action required.

PdraRxTopoHidingApplied

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of messages received on Rx interface on which topology hiding has been applied by P-DRA.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented each time topology hiding is applied when a message from Rx interface is processed by the application.
Measurement Scope: All
Recovery:
No action necessary.

RxBindCapApn2PcrfPool

Measurement Group: P-DRA Diameter Usage
Description: The number of times a given APN is successfully mapped to PCRF pool.
Measurement Type: Simple
Measurement Dimension: Arrayed (by APN)
Collection Interval: 5 min
Peg Condition: Each time a binding capable session initiation request is successfully mapped to a PCRF Pool (a configured APN), regardless of whether or not the rule matching results in the selection of a PCRF Pool or a PCRF Sub-Pool.
Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association
Recovery:
1. This measurement shows the distribution of binding capable session initiation requests across the range of configured APNs.
2. Contact My Oracle Support (MOS).

RxBindCapPcrfPool2Prt

Measurement Group: P-DRA Diameter Usage
Description: The number of binding capable session initiation requests that are routed using a PRT table chosen as a result of PCRF Pool or PCRF Sub-Pool mapping to the PRT.
Measurement Type: Simple
Measurement Dimension: Arrayed (by PCRF Pool or Sub-Pool)
Collection Interval: 5 min
Peg Condition: Each time a binding capable session initiation request is routed using a PRT table selected on the basis of the PCRF Pool or Sub-Pool, regardless of whether or not the request was routed successfully.
Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association
Recovery:
1. This measurement shows the distribution of binding capable session initiation requests that are routed using a given Peer Routing Table at each site.
2. Contact My Oracle Support (MOS).

RxBindCap2PcrfSubPool
Measurement Group: P-DRA Diameter Usage
Description: The number of binding capable session initiation requests that were mapped to a PCRF Sub-Pool by a given PCRF Sub-Pool Selection Rule.
Measurement Type: Simple
Measurement Dimension: Arrayed (by PCRF Sub-Pool Selection Rule)
Collection Interval: 5 min
Peg Condition: Each time a binding capable session initiation request is successfully mapped to a PCRF Sub-Pool as a result of a given PCRF Sub-Pool Selection Rule, regardless of whether the request is routed to the Sub-Pool or routed elsewhere due to an existing binding.
Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association
Recovery:
1. This measurement shows the distribution of binding capable session initiation requests for which a new binding would route to a PCRF Sub-Pool across the set of PCRF Sub-Pool Selection Rules.
2. Contact My Oracle Support (MOS).

RxCCRInitNoImsiMsgs
Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of CCR Initial messages without IMSI.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented each time P-DRA processes a CCR Initial message in which IMSI is not present.
Measurement Scope: All
Recovery:
Measurements

No action necessary.

RxPdra5002FromPcrf

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a PCRF
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time a PCRF responds to a Diameter request with a 5002 response code.
Measurement Scope: All
Recovery:
   No action necessary.

RxPdra5002FromPolicyClient

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a policy client.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time a policy client responds to a Diameter request with a 5002 response code.
Measurement Scope: All
Recovery:
   No action necessary.

RxPdraAarMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of AAR messages received by PDRA.
Collection Interval: 5 min
**Peg Condition:** The measurement shall be incremented each time the application receives an AAR message.

**Measurement Scope:** All

**Recovery:**

No action necessary.

**RxPdraAsrMsgs**

**Measurement Group:** P-DRA Diameter Usage

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of ASR messages received by PDRA.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented each time the application receives an ASR message.

**Measurement Scope:** All

**Recovery:**

No action necessary.

**RxPdraCcrInitMsgs**

**Measurement Group:** P-DRA Diameter Usage

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of CCR Initial messages received by PDRA.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented each time the application receives a CCR Initial message.

**Measurement Scope:** All

**Recovery:**

No action necessary.

**RxPdraCcrTerminateMsgs**

**Measurement Group:** P-DRA Diameter Usage

**Measurement Type:** Simple

**Measurement Dimension:** Single
Measurements

RxPdraCcrUpdateMsgs

- **Measurement Group**: P-DRA Diameter Usage
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: Number of CCR Update messages received by PDRA.
- **Collection Interval**: 5 min
- **Peg Condition**: The measurement shall be incremented each time the application receives a CCR Update message.
- **Measurement Scope**: All
- **Recovery**: No action necessary.

GxpBindingSuccess

- **Measurement Group**: P-DRA Diameter Usage
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: Number of Gx-Prime CCR Initial messages processed by P-DRA against binding key priorities.
- **Collection Interval**: 5 min
- **Peg Condition**: Each time a Gx-Prime CCR-I message is processed by P-DRA.
- **Note**: The number is sorted and stored in 5 buckets:
  - Bucket 1 holds the number of Gx-Prime CCR-I messages that lead to successful binding record findings corresponding to the binding keys with the highest (1) priority.
  - Bucket 2 (or 3 or 4) holds the number of Gx-Prime CCR-I messages that lead to successful binding record findings corresponding to the configured binding keys with priority 2 (or 3 or 4).
  - Bucket 5 holds the number of Gx-Prime CCR-I messages that lead NO binding record finding after exhausting all binding keys.
- **Measurement Scope**: All
Measurements

Recovery:
No action required.

RxPdraGxpCcrInitMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Gx-Prime CCR Initial messages processed by P-DRA.
Collection Interval: 5 min
Peg Condition: Each time a Gx-Prime CCR-I message is processed by P-DRA.
Measurement Scope: All
Recovery:
No action required.

RxPdraGxpCcrUpdateMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Gx-Prime CCR Update messages processed by P-DRA against binding key priorities.
Collection Interval: 5 min
Peg Condition: Each time the P-DRA Application receives a Gx-Prime CCR Update message.
Measurement Scope: All
Recovery:
No action required.

RxPdraGxpCcrTerminateMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Gx-Prime CCR Termination messages received by P-DRA against binding key priorities.
Collection Interval: 5 min
Peg Condition: Each time the P-DRA Application receives a Gx-Prime CCR Termination message.
Measurements

Measurement Scope: All
Recovery: No action required.

RxPdraMsgRateAvg

Measurement Group: P-DRA Diameter Usage
Measurement Type: Average
Measurement Dimension: Single
Description: Average Diameter ingress message processing rate of P-DRA during the collection interval.
Collection Interval: 5 min
Peg Condition: This peg is periodically updated based on average rate of the Diameter ingress messages being processed by P-DRA calculated over the collection interval.
Measurement Scope: All
Recovery: No action necessary.

RxPdraMsgRatePeak

Measurement Group: P-DRA Diameter Usage
Measurement Type: Max
Measurement Dimension: Single
Description: Peak Diameter ingress message processing rate of P-DRA during the collection interval.
Collection Interval: 5 min
Peg Condition: This peg is periodically updated based on maximum rate of the Diameter ingress messages being processed by P-DRA calculated over the collection interval.
Measurement Scope: All
Recovery: No action necessary.

RxPdraRarGxMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of RAR messages received by PDRA for Gx interface,
Measurements

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives a RAR message for Gx interface.

Measurement Scope: All

Recovery: No action necessary.

RxPdraRarGxpMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Gx-Prime RAR messages processed by P-DRA.
Collection Interval: 5 min
Peg Condition: Each time a Gx-Prime RAR message is processed by P-DRA.
Measurement Scope: All
Recovery: No action required.

RxPdraRarRxMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of RAR messages received by PDRA for Rx interface.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented each time the application receives a RAR message for Rx interface.
Measurement Scope: All
Recovery: No action necessary.

RxPdraStrMsgs

Measurement Group: P-DRA Diameter Usage
Measurement Type: Simple
Measurement Dimension: Single
**Description:** Number of STR messages received by PDRA.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented per interface each time the application receives a STR message.

**Measurement Scope:** All

**Recovery:**

No action necessary.

---

**TxPdraGxRarQuery**

**Measurement Group:** P-DRA Diameter Usage

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of Gx RAR messages initiated by P-DRA for the purposes of querying for session existence at the policy client.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented by one each time a P-DRA DA-MP server sends a P-DRA initiated RAR request to a policy client for the purpose of querying the policy client for session existence.

**Measurement Scope:** All

**Recovery:**

1. If this value is consistently non-zero, it may indicate that the stale session timing is configured to be too short. The stale session timer for a given session is configured in **Policy DRA > Configuration > Access Point Names** if the session is associated with a configured APN, or **Policy DRA > Configuration > Network-Wide Options** if the session is not associated with an APN, or associated with an APN that is not configured.

2. If the problem persists, contact **My Oracle Support (MOS)**.

---

**TxPdraGxRarRelease**

**Measurement Group:** P-DRA Diameter Usage

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of Gx RAR requests initiated by P-DRA for the purpose of releasing a session as a result of an error in the P-DRA.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be pegged each time a P-DRA DA-MP server sends a P-DRA initiated RAR request to a policy client for the purpose of releasing a session due to an error in the P-DRA

**Measurement Scope:** All
Recovery:

1. Check Alarms & Events > View History GUI for pSBR event 22711 - Policy SBR Database Error for more details about the possible cause of the error.
2. Contact My Oracle Support (MOS) for support as needed.

P-DRA Diameter Exception measurements

The P-DRA Diameter Exception measurement report contains measurements that provide performance information that is specific to the P-DRA Diameter protocol.

Table 72: P-DRA Diameter Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxBindCapPcrfPoolNotMapped</td>
<td>Number of binding capable session initiation requests that were destined for a PCRF Pool or Sub-Pool for which no PRT table was configured</td>
<td>5 min</td>
</tr>
<tr>
<td>RxBindCapUnknownApn</td>
<td>Number of binding capable session initiation requests containing an unconfigured APN</td>
<td>5 min</td>
</tr>
<tr>
<td>RxBindCapMissingApn</td>
<td>Number of binding capable session initiation requests containing no APN</td>
<td>5 min</td>
</tr>
<tr>
<td>RxBindDepUnknownApn</td>
<td>Number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing an unconfigured APN</td>
<td>5 min</td>
</tr>
<tr>
<td>RxBindDepMissingApn</td>
<td>Number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing no APN</td>
<td>5 min</td>
</tr>
<tr>
<td>RxBindCapUnknownPcrf</td>
<td>Number of binding capable session initiation answers coming from an unconfigured PCRF</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPdraRequestProtocolErr</td>
<td>Number of invalid Request messages received from DRL. Invalid request message includes - unsupported command codes, unsupported application Id, missing or invalid AVPs.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxStackEventDiscardedCaFailure</td>
<td>Number of stack events discarded by ComAgent due to ComAgent failures</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TxAaxMsgDiscardedDueToDrlQueueFull</td>
<td>Number of AAR/AAA messages discarded by P-DRA due to DRL queue being full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxAsxMsgDiscardedDueToDrlQueueFull</td>
<td>Number of ASR messages discarded by P-DRA due to DRL queue being full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxCcxMsgDiscardedDueToDrlQueueFull</td>
<td>Number of CCR/CCA messages discarded by P-DRA due to DRL queue being full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPdraAnswersGeneratedForDiameterErr</td>
<td>Number of Diameter answers generated by P-DRA due to error in received Diameter messages from DRL.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPdraAnswersGeneratedForPsrbErrResp</td>
<td>Number of Diameter Answer messages generated by P-DRA because of pSBR stack event error response.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPdraAnswersGeneratedConfigErr</td>
<td>Number of Diameter Answers generated by P-DRA due to configuration errors when processing session initiation requests.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPdraErrAnsGeneratedCAFailure</td>
<td>Number of Diameter answers generated by P-DRA due to ComAgent failure.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxGxpCcxMsgDiscardedDrlQueueFull</td>
<td>Number of Gx-Prime CCR/CCA messages discarded by P-DRA due to the DRL queue being full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxRaxMsgDiscardedDueToDrlQueueFull</td>
<td>Number of RAR/RAA messages discarded by P-DRA due to DRL queue being full.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxStxMsgDiscardedDueToDrlQueueFull</td>
<td>Number of STR/STA messages discarded by P-DRA due to DRL queue being full.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxBindCapPcrfPoolNotMapped**

**Measurement Group:** P-DRA Diameter Exception

**Description:** The number of binding capable session initiation requests that were destined for a PCRF Pool or Sub-Pool for which no PRT table was configured.

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Collection Interval:** 5 min
**Peg Condition:** Each time a new binding attempt is supposed to be routed to a PCRF Pool or Sub-Pool for which no PRT table is configured at the site where the routing is occurring.

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**

1. This measurement represents an exception condition in which a PCRF Pool or Sub-Pool has been configured for use at the NOAMP, but no PRT table has been configured at one or more sites to route requests to that PCRF Pool or Sub-Pool. Consider whether a PRT table should be configured at the Network Element to which this measurement applies.
2. Contact *My Oracle Support (MOS).*

**RxBindCapUnknownApn**

**Measurement Group:** P-DRA Diameter Exception

**Description:** The number of binding capable session initiation requests containing an unconfigured APN.

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Collection Interval:** 5 min

**Peg Condition:** Each time a binding capable session initiation request is received containing an APN that is not configured at the Policy DRA NOAMP.

**Note:** This condition also causes **22730 - Policy DRA Configuration Error** to be asserted.

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**

1. This measurement represents an exception condition in which binding capable session initiation request are being received from unknown APN values. Each binding capable session initiation request containing an unconfigured APN is rejected using the Missing Or Unconfigured APN error condition.
2. Contact *My Oracle Support (MOS).*

**RxBindCapMissingApn**

**Measurement Group:** P-DRA Diameter Exception

**Description:** The number of binding capable session initiation requests containing no APN.

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Collection Interval:** 5 min

**Peg Condition:** Each time a binding capable session initiation request is received containing no APN (i.e. no Called-Station-ID AVP).

**Note:** This condition also causes **22730 - Policy DRA Configuration Error** to be asserted.
Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which binding capable session initiation request are being received with no APN value. Each binding capable session initiation request containing a missing APN is rejected using the Missing Or Unconfigured APN error condition.
2. Contact My Oracle Support (MOS).

**RxBindDepUnknownApn**

**Measurement Group:** P-DRA Diameter Exception

**Description:** The number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing an unconfigured APN.

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Collection Interval:** 5 min

**Peg Condition:** Each time an attempt is made to find a binding using either IMSI or MSISDN, but the binding dependent session initiation request contains an APN that is not configured at the Policy DRA NOAMP. If both IMSI and MSISDN are configured in the binding key priority table, this measurement can be incremented twice for one binding dependent session initiation request.

**Note:** This condition also causes 22730 - Policy DRA Configuration Error to be asserted.

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**

1. This measurement represents an exception condition in which the binding key priority is configured to use IMSI, MSISDN, or both, but the binding dependent session initiation request has an APN value that is not configured. This condition causes binding correlation to fail for the MSISDN or IMSI key types. If no other key is present and configured for correlation, the request is rejected using the Binding Not Found error condition.
2. Contact My Oracle Support (MOS).

**RxBindDepMissingApn**

**Measurement Group:** P-DRA Diameter Exception

**Description:** The number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing no APN.

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Collection Interval:** 5 min

**Peg Condition:** Each time an attempt is made to find a binding using either IMSI or MSISDN, but the binding dependent session initiation request contains no APN. If both IMSI and MSISDN are configured in the binding key priority table, this measurement can be incremented twice for one binding dependent session initiation request.
Note: This condition also causes 22730 - Policy DRA Configuration Error to be asserted.

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**

1. This measurement represents an exception condition in which the binding key priority is configured to use IMSI, MSISDN, or both, but the binding dependent session initiation request has no APN value. This condition causes binding correlation to fail for the MSISDN or IMSI key types. If no other key is present and configured for correlation, the request is rejected using the Binding Not Found error condition.
2. Contact *My Oracle Support (MOS).*

**RxBindCapUnknownPcrf**

**Measurement Group:** P-DRA Diameter Exception

**Description:** The number of binding capable session initiation answers coming from an unconfigured PCRF.

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Collection Interval:** 5 min

**Peg Condition:** Each time a binding capable session initiation answer for a new binding is received from a PCRF that is not configured at the Policy DRA SOAM.

Note: This condition also causes 22730 - Policy DRA Configuration Error to be asserted.

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**

1. This measurement represents an exception condition in which binding capable session initiation answers for new bindings are being received from unknown PCRF FQDNs. When this occurs, the binding capable session answered by the unconfigured PCRF is torn down by an RAR containing a Session-Release-Cause AVP send from the Policy DRA.
2. Refer to 22730 - Policy DRA Configuration Error for further information.
3. Contact *My Oracle Support (MOS).*

**RxPdraRequestProtocolErr**

**Measurement Group:** P-DRA Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of invalid Request messages received from DRL. Invalid request message includes - unsupported command codes, unsupported application Id, missing or invalid AVPs. The AARs without Dest-Host AVP are still valid AARs and shall be pegged.

**Collection Interval:** 5 min
**Peg Condition:** The measurement shall be incremented by one each time an invalid diameter request message is received by P-DRA.

**Measurement Scope:** All

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance.

**RxStackEventDiscardedCaFailure**

**Measurement Group:** P-DRA Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of stack events discarded by ComAgent due to ComAgent failure.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented by one each time a stack event is discarded by ComAgent due to a ComAgent failure as indicated by a returned stack event error code of all available error codes.

**Measurement Scope:** All

**Recovery:**

1. Check ComAgent event 19832 - *Communication Agent Reliable Transaction Failed* and ComAgent measurements CAHSTxDscrdCongSR, CAHSTxDscrdUnkwnRsrc, and CAHSTxDscrdIntErrSR for detailed error causes.
2. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

**TxAaxMsgDiscardedDueToDrlQueueFull**

**Measurement Group:** P-DRA Diameter Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of AAR/AAA messages discarded by P-DRA due to DRL queue being full.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented by one each time a AAR/AAA message is discarded by the application because DRL queue is full.

**Measurement Scope:** All

**Recovery:**

No action required.

**TxAsxMsgDiscardedDueToDrlQueueFull**

**Measurement Group:** P-DRA Diameter Exception
Measurements

Measurement Type: Simple
Measurement Dimension: Single
Description: Number of ASR messages discarded by P-DRA due to DRL queue being full.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented by one each time a ASR message is discarded by the application because DRL queue is full.
Measurement Scope: All
Recovery: No action required.

TxCcxMsgDiscardedDueToDrlQueueFull
Measurement Group: P-DRA Diameter Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of CCR/CCA messages discarded by P-DRA due to DRL queue being full.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented by one each time a CCR/CCA message is discarded by the application because DRL queue is full.
Measurement Scope: All
Recovery: No action required.

TxPdraAnswersGeneratedForDiameterErr
Measurement Group: P-DRA Diameter Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Diameter answers generated by P-DRA due to error in received Diameter messages from DRL.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented by one each time a diameter answer message is generated by P-DRA due to error in received Diameter messages from DRL.
The errors encountered may be:
• Diameter protocol errors
• P-DRA application specific errors due to absence of some optional AVP(s) in the Diameter request
Measurement Scope: All
Recovery:
No action required.

TxPdraAnswersGeneratedForPsbrErrResp

Measurement Group: P-DRA Diameter Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of Diameter Answer messages generated by P-DRA because of pSBR stack event error response.
Collection Interval: 5 min
Peg Condition: The measurement shall be incremented by one each time a diameter answer message is generated by P-DRA because of pSBR stack event error response.
Measurement Scope: All
Recovery: No action required.

TxPdraAnswersGeneratedConfigErr

Measurement Group: P-DRA Diameter Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Diameter Answers generated by P-DRA due to configuration errors when processing binding capable session initiation requests.
Collection Interval: 5 min
Peg Condition: This measurement is pegged each time when P-DRA generates an error Answer in processing a binding capable session initiation request due to
- No PCRF being configured at the site where the request is processed OR
- No PCRF ID being found in PCRF table OR
- The APN contained in the request message not configured.
The measurement is pegged also each time when P-DRA generates an error Answer in processing a binding dependent session initiation request if the APN in the request is not configured in the Policy DRA and the site is configured to correlate on IMSI, MSISDN, or both and no other binding correlation key is successfully used for correlation.
Note: In binding dependent request cases, this measurement is raised only when the Binding Not Found condition applies, the APN is unconfigured, and an IMSI or MSISDN was used as a possible correlation key.
Measurement Scope: All
Recovery:
1. Check the P-DRA System OAM GUI Main Menu: **Policy DRA > Configuration > PCRFs** to ensure PCRFs are configured properly.

2. 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 DRA > Configuration > 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 DRA > Configuration > PCRFs**. If the PCRF is not valid for the request, correct the routing table or tables that included the PCRF.

   See also **RxBindCapUnknownPcrf**.

3. If there is an unconfigured APN and if the APN string is valid, configure the APN at the NOAMP using the **Policy DRA > 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.

   See also **RxBindCapUnknownApn** and **RxBindDepUnknownApn**.

4. If there is a missing APN, investigate the policy client to determine why it is sending policy session initiation requests with no APN.

   See also **RxBindCapMissingApn** and **RxBindDepMissingApn**

5. If there are no PCRFs configured, configure PCRFs at the SOAM GUI for the site using **Policy DRA > Configuration > PCRFs**.

6. If needed, contact **My Oracle Support (MOS)** for further assistance.

---

### Measurements

1. **TxPdraErrAnsGeneratedCAFailure**
   - **Measurement Group**: P-DRA Diameter Exception
   - **Measurement Type**: Simple
   - **Measurement Dimension**: Single
   - **Description**: Number of Diameter answers generated by P-DRA due to ComAgent failure.
   - **Collection Interval**: 5 min
   - **Peg Condition**: The measurement shall be incremented by one each time a diameter answer message is generated by P-DRA due to comagent routing failure.
   - **Measurement Scope**: All
   - **Recovery**: No action required.

2. **TxGxpCcxMsg DiscordedDrlQueueFull**
   - **Measurement Group**: P-DRA Diameter Exception
   - **Measurement Type**: Simple
   - **Measurement Dimension**: Single
   - **Description**: Number of Gx-Prime CCR/CCA messages discarded by P-DRA due to DRL queue being full.
Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime CCR/CCA message is discarded by the P-DRA application because DRL queue is full.

Measurement Scope: All

Recovery:

   Contact *My Oracle Support (MOS)*.

**TxRaxMsgDiscardedDueToDrlQueueFull**

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of RAR/RAA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a RAR/RAA message is discarded by the application because DRL queue is full. The measurement shall be incremented by one each time a CCR/CCA message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

   No action required.

**TxStxMsgDiscardedDueToDrlQueueFull**

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Description: Number of STR/STA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a STR/STA message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

   No action required.

**P-DRA Congestion Exception measurements**

The P-DRA Congestion Exception measurement report contains measurements that provide performance information that is specific to the P-DRA Diameter protocol.
Table 73: P-DRA Congestion Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxAarMsgDiscardedDueToCongestion</td>
<td>Number of AAR messages discarded by P-DRA due to congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxAsrMsgDiscardedDueToCongestion</td>
<td>Number of ASR messages discarded by P-DRA due to P-DRA congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxCcrMsgDiscardedDueToCongestion</td>
<td>Number of CCR messages discarded by P-DRA due to congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxGxpCcrMsgDiscardedDueToCongestion</td>
<td>Number of Gx-Prime CCR messages discarded by P-DRA due to P-DRA internal congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRarMsgDiscardedDueToCongestion</td>
<td>Number of RAR messages discarded by P-DRA due to congestion.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxStrMsgDiscardedDueToCongestion</td>
<td>Number of STR messages discarded by P-DRA due to congestion.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxAarMsgDiscardedDueToCongestion**

**Measurement Group:** P-DRA Congestion Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of AAR messages discarded by P-DRA due to congestion.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented by one each time an AAR message is discarded by P-DRA due to congestion.

**Measurement Scope:** All

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance.

**RxAsrMsgDiscardedDueToCongestion**

**Measurement Group:** P-DRA Congestion Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of ASR messages discarded by P-DRA due to P-DRA congestion.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented by one each time an ASR message is discarded by P-DRA due to congestion.
**Measurement Scope:** All
**Recovery:**
Contact *My Oracle Support (MOS)* for assistance.

**RxCcrMsgDiscardedDueToCongestion**

**Measurement Group:** P-DRA Congestion Exception
**Measurement Type:** Simple
**Measurement Dimension:** Single
**Description:** Number of CCR messages discarded by P-DRA due to congestion.
**Collection Interval:** 5 min
**Peg Condition:** The measurement shall be incremented by one each time a CCR message is discarded by P-DRA due to congestion.

**Measurement Scope:** All
**Recovery:**
Contact *My Oracle Support (MOS)* for assistance.

**RxGxpCcrMsgDiscardedDueToCongestion**

**Measurement Group:** P-DRA Diameter Exception
**Measurement Type:** Simple
**Measurement Dimension:** Single
**Description:** Number of Gx-Prime CCR messages discarded by P-DRA due to P-DRA internal congestion.
**Collection Interval:** 5 min
**Peg Condition:** Each time a Gx-Prime CCR message is discarded by the P-DRA application due to P-DRA internal congestion.

**Measurement Scope:** All
**Recovery:**
Contact *My Oracle Support (MOS)* for assistance.

**RxRarMsgDiscardedDueToCongestion**

**Measurement Group:** P-DRA Congestion Exception
**Measurement Type:** Simple
**Measurement Dimension:** Single
**Description:** Number of RAR messages discarded by P-DRA due to congestion.
Collection Interval: 5 min

**Peg Condition:** The measurement shall be incremented by one each time an RAR message is discarded by P-DRA due to congestion.

**Measurement Scope:** Network, NE, Server

**Recovery:**
Contact *My Oracle Support (MOS)* for assistance.

**RxStrMsgDiscardedDueToCongestion**

**Measurement Group:** P-DRA Congestion Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** Number of STR messages discarded by P-DRA due to congestion.

**Collection Interval:** 5 min

**Peg Condition:** The measurement shall be incremented by one each time an STR message is discarded by P-DRA due to congestion.

**Measurement Scope:** All

**Recovery:**
Contact *My Oracle Support (MOS)* for assistance.

**pSBR Binding Performance measurements**

The pSBR Binding Performance measurement report contains measurements that provide performance information that is specific to the pSBR Binding Database.

**Table 74: pSBR Binding Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrNewBindingsCreated</td>
<td>The number of new bindings created.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrUpdatedBindings</td>
<td>The number of existing bindings updated but not deleted</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrBindTermByAscSess</td>
<td>The number bindings (final) terminated due to termination of all associated sessions.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAltKeyCreated</td>
<td>The number of alternate key records created.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAltKeyDel</td>
<td>The number of alternate key records removed.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>PsbrMaxBindingAgeAtTerm</td>
<td>The average binding (final) age when binding is terminated due to termination of all associated sessions</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAvgBindingAgeAtTerm</td>
<td>The maximum binding (final) age when binding is terminated due to termination of all associated sessions.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAvgBindingDbRead</td>
<td>The average rate of Binding database reads per second</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMaxBindingDbRead</td>
<td>The maximum rate of Binding database reads</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAvgBindingDbWrite</td>
<td>The average rate of Binding database writes per second</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMaxBindingDbWrite</td>
<td>The maximum rate of Binding database writes</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrEarlySlaveBindingsCreated</td>
<td>The number of binding capable session initiation requests that were treated as slaves of an existing early binding</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrFinalBindingsFollowed</td>
<td>The number of binding capable session initiation requests for which an existing final binding existed</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSlavePollingContinue</td>
<td>The number of early binding polling attempts for which the poller was instructed to continue polling</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSlavePollingRouteToPcrf</td>
<td>The number of early binding polling attempts for which the poller was instructed to route to a final binding</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrLockCollisions</td>
<td>The number of collisions occured periodically while acquiring a lock.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmPsbrProcessingTime</td>
<td>Time (in microseconds) to process an event on pSBR. The measurement is to measure the average time (ms) taken for pSBR to process the stack event received from P-DRA and send back the stack event response to P-DRA.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
PsbrNewBindingsCreated

Measurement Group: pSBR Binding Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of new bindings created.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a new binding is created.
Measurement Scope: Place Association
Recovery:
  No action necessary.

PsbrUpdatedBindings

Measurement Group: pSBR Binding Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of existing bindings updated but not deleted, i.e. the Session Reference removed is not the last one
Collection Interval: 5 min
Peg Condition: This peg is updated whenever an existing binding is updated.
Measurement Scope: Place Association
Recovery:
  No action necessary.

PsbrBindTermByAscSess

Measurement Group: pSBR Binding Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number bindings (final) terminated due to termination of all associated sessions.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a binding is terminated due to termination of all associated sessions.
Measurement Scope: Place Association
Recovery:
No action necessary.

**PsbrAltKeyCreated**
- **Measurement Group:** pSBR Binding Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of alternate key records created.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever an alternate key record is created.
- **Measurement Scope:** Place Association
- **Recovery:**
  - No action necessary.

**PsbrAltKeyDel**
- **Measurement Group:** pSBR Binding Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of alternate key records removed.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever an alternate key record is deleted.
- **Measurement Scope:** Place Association
- **Recovery:**
  - No action necessary.

**PsbrMaxBindingAgeAtTerm**
- **Measurement Group:** pSBR Binding Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The maximum binding (final) age when binding is terminated due to termination of all associated sessions.
- **Collection Interval:** 5 min
- **Peg Condition:** The time interval starts when the binding becomes final and stops when binding is terminated due to termination of all associated sessions.
- **Measurement Scope:** Place Association
Recovery:
  No action necessary.

PsbrAvgBindingAgeAtTerm
  Measurement Group: pSBR Binding Performance
  Measurement Type: Average
  Measurement Dimension: Single
  Description: The average binding (final) age when binding is terminated due to termination of all associated sessions.
  Collection Interval: 5 min
  Peg Condition: The time interval starts when the binding becomes final and stops when binding is terminated due to termination of all associated sessions.
  Measurement Scope: All
  Recovery: No action necessary.

PsbrAvgBindingDbRead
  Measurement Group: pSBR Binding Performance
  Measurement Type: Average
  Measurement Dimension: Single
  Description: The average rate of Binding database reads per second
  Collection Interval: 5 min
  Peg Condition: It is calculated based on the total number of sampled binding database reads during the collection interval.
  Measurement Scope: All
  Recovery: No action necessary.

PsbrMaxBindingDbRead
  Measurement Group: pSBR Binding Performance
  Measurement Type: Max
  Measurement Dimension: Single
  Description: The maximum rate of Binding database reads
  Collection Interval: 5 min
Peg Condition: At the end of each sample period associated with the average binding database reads, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: All

Recovery:
No action necessary.

PsbrAvgBindingDbWrite

Measurement Group: pSBR Binding Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average rate of Binding database writes per second
Collection Interval: 5 min

Peg Condition: It is calculated based on the total number of sampled binding database writes during the collection interval.

Measurement Scope: All

Recovery:
No action necessary.

PsbrMaxBindingDbWrite

Measurement Group: pSBR Binding Performance
Measurement Type: Max
Measurement Dimension: Single
Description: The maximum rate of Binding database writes
Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with the average binding database writes, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: All

Recovery:
No action necessary.

PsbrEarlySlaveBindingsCreated

Event Group: pSBR Binding Performance
Description: The number of binding capable session initiation requests that were treated as slaves of an existing early binding.
Measurement Type: Simple  
Measurement Dimension: Single  
Collection Interval: 5 min  
Peg Condition: Each time a binding capable session initiation request is received and all of the following conditions are true:
  • The CCR-I matches an existing binding that is in the Early state (i.e. there exists an EarlyMaster sessionRef for the IMSI and APN, or IMSI and PCRF Pool)  
  • The existing EarlyMaster sessionRef has not been in existence for longer than the Maximum Early Binding Lifetime configured in Policy DRA > Configuration > Network-Wide Options  
  • PCRF Pooling is Enabled  
Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association  
Recovery:  
  1. This measurement gives an indication of the frequency at which the early binding mechanism is being exercised.  
  2. Contact My Oracle Support (MOS).

PsbrFinalBindingsFollowed  
Event Group: pSBR Binding Performance  
Description: A count of the number of binding capable session initiation requests that matched a final binding and were routed using the bound PCRF.  
Measurement Type: Simple  
Measurement Dimension: Single  
Collection Interval: 5 min  
Peg Condition: Each time a binding capable session initiation request is received and all of the following conditions are true:
  • The CCR-I matches an existing binding that is in the Final state (i.e. there exists a Final sessionRef for the IMSI and APN, or IMSI and PCRF Pool)  
  • PCRF Pooling is Enabled  
Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association  
Recovery:  
  1. This measurement gives an indication of the frequency at which binding capable session initiation requests are routed according to existing bindings.  
  2. Contact My Oracle Support (MOS).

PsbrSlavePollingContinue  
Measurement Group: pSBR Binding Performance  
Description: A count of the number of early binding polling attempts for which the poller was instructed to continue polling.
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Collection Interval:** 5 min  
**Peg Condition:** Each time an Early Binding Slave session polls the Early Binding Master and all of the following conditions are true:  
- The Early Binding Master sessionRef still exists in the binding database and is in the EarlyMaster state.  
- The Early Binding Slave sessionRef still exists in the binding database  
- The Early Binding Master sessionRef has not been in existence for longer than the Maximum Early Binding Lifetime  
- PCRF Pooling is Enabled  
**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association  
**Recovery:**  
1. This measurement gives an indication of the frequency at slave pollers are asked to continue polling. If this value is equal to or higher than the PsbrEarlySlaveBindingsCreated, the Early Binding Polling Interval configured in **Policy DRA > Configuration > Network-Wide Options** may be set to a duration too short, causing unnecessary polling attempts. If this value is very low relative to the PsbrEarlySlaveBindingsCreated, the Early Binding Polling Interval may be set to a duration too long, causing unnecessary latency for slave sessions.  
2. Contact **My Oracle Support (MOS).**

**PsbrSlavePollingRouteToPcrf**

**Measurement Group:** pSBR Binding Performance  
**Description:** A count of the number of early binding polling attempts for which the poller was instructed to route the request to a bound PCRF.  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Collection Interval:** 5 min  
**Peg Condition:** Each time an Early Binding Slave session polls the Early Binding Master and all of the following conditions are true:  
- The Early Binding Master sessionRef still exists in the binding database and is in the Final state.  
- The Early Binding Slave sessionRef still exists in the binding database  
- PCRF Pooling is Enabled  
**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association  
**Recovery:**  
1. This measurement gives an indication of the Early Binding Slave sessions whose master sessionRefs became Final and were therefore routed using the bound PCRF. If this value is lower than the PsbrEarlySlaveBindingsCreated value, check the pSBR Binding Exception measurement report for measurement PsbrSlavePollingFail.  
2. Contact **My Oracle Support (MOS).**
PsbrLockCollisions

- **Measurement Group**: pSBR Binding Performance
- **Measurement Type**: Simple
- **Measurement Dimension**: Arrayed
- **Description**: The number of collisions that occurred periodically while acquiring a lock
- **Collection Interval**: 5 min
- **Peg Condition**: Each time a collision occurs while acquiring a lock
- **Measurement Scope**: All
- **Recovery**: No action necessary.

TmPsbrProcessingTime

- **Measurement Group**: pSBR Binding Performance
- **Measurement Type**: Simple
- **Measurement Dimension**: Arrayed
- **Description**: The time (in microseconds) to process an event on pSBR. The measurement is to measure the average time (ms) taken for pSBR to process the stack event received from P-DRA and send back the stack event response to P-DRA.
- **Collection Interval**: 5 min
- **Peg Condition**: Each time a stack event is received from P-DRA and is sent back the response to P-DRA
- **Measurement Scope**: All
- **Recovery**: No action necessary.

**pSBR Session Performance measurements**

The pSBR Binding Performance measurement report contains measurements that provide performance information that is specific to the pSBR Session Database.

**Table 75: pSBR Session Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrSessionsCreated</td>
<td>The number of new sessions created.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSessionsRefresh</td>
<td>The number of existing sessions refreshed.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

E53474 Revision 01, July 2014
<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrSessionsDeleted</td>
<td>The number of sessions removed.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAvgSessionAgeTermPerAPN</td>
<td>The average time interval (in hours) per APN betwen the time when a session record is created and the time when it is successfully terminated.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMaxSessionAgeTermPerAPN</td>
<td>The maximum time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAvgSessionDbRead</td>
<td>The average rate of Session database reads per second</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMaxSessionDbRead</td>
<td>At the end of each sample period associated with the average session database reads, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrAvgSessionDbWrite</td>
<td>The average rate of session database writes per second</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMaxSessionDbWrite</td>
<td>The maximum rate of session database writes</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrPendingRarLockCollisions</td>
<td>The number of collisions occurred periodically while acquiring a lock to update PendingRar table.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**PsbrSessionsCreated**

**Measurement Group:** pSBR Session Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of new sessions created.  
**Collection Interval:** 5 min  
**Peg Condition:** This peg is updated whenever a new session is created.  
**Measurement Scope:** All  
**Recovery:**  
No action necessary.
PsbrSessionsRefresh

Measurement Group: pSBR Session Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of existing sessions refreshed.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever an existing session is refreshed.
Measurement Scope: All
Recovery:
   No action necessary.

PsbrSessionsDeleted

Measurement Group: pSBR Session Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of sessions removed.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a session is deleted.
Measurement Scope: All
Recovery:
   No action necessary.

PsbrAvgSessionAgeTermPerAPN

Measurement Group: pSBR Session Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.
Collection Interval: 5 min
Peg Condition: The time interval starts when a session record is created as a result of createSession stack event and stops when the session record is terminated successfully as a result of removeSession stack event
Measurement Scope: All
Recovery:
No action necessary.

**PsbrMaxSessionAgeTermPerAPN**

- **Measurement Group:** pSBR Session Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** The maximum time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.
- **Collection Interval:** 5 min
- **Peg Condition:** The time interval starts when a session record is created as a result of createSession stack event and stops when the session record is terminated successfully as a result of removeSession stack event
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrAvgSessionDbRead**

- **Measurement Group:** pSBR Session Performance
- **Measurement Type:** Average
- **Measurement Dimension:** Single
- **Description:** The average rate of Session database reads per second
- **Collection Interval:** 5 min
- **Peg Condition:** It is calculated based on the total number of sampled session database reads during the collection interval.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrMaxSessionDbRead**

- **Measurement Group:** pSBR Session Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The maximum rate of Session database reads
- **Collection Interval:** 5 min
**Peg Condition:** At the end of each sample period associated with the average session database reads, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value

**Measurement Scope:** All

**Recovery:**
No action necessary.

**PsbrAvgSessionDbWrite**

**Measurement Group:** pSBR Session Performance

**Measurement Type:** Average

**Measurement Dimension:** Single

**Description:** The average rate of session database writes per second

**Collection Interval:** 5 min

**Peg Condition:** It is calculated based on the total number of sampled session database writes during the collection interval.

**Measurement Scope:** All

**Recovery:**
No action necessary.

**PsbrMaxSessionDbWrite**

**Measurement Group:** pSBR Session Performance

**Measurement Type:** Max

**Measurement Dimension:** Single

**Description:** The maximum rate of session database writes

**Collection Interval:** 5 min

**Peg Condition:** At the end of each sample period associated with the average session database writes, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.

**Measurement Scope:** All

**Recovery:**
No action necessary.

**PsbrPendingRarLockCollisions**

**Measurement Group:** pSBR Session Performance

**Measurement Type:** Simple
**Measurement Dimension:** Arrayed

**Description:** The number of collisions occurred periodically while acquiring a lock to update PendingRar table.

**Collection Interval:** 5 min

**Peg Condition:** Each time a collision occurs while acquiring a lock to update PendingRar table.

**Measurement Scope:** All

**Recovery:**
No action necessary.

### pSBR Binding Exception measurements

The pSBR Binding Exception measurement report contains measurements that provide performance information that is specific to the pSBR Binding Database.

**Table 76: pSBR Binding Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrCreateBindDbErr</td>
<td>The number of errors creating a binding record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrUpdateBindDbErr</td>
<td>The number of errors updating a binding record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrRemoveBindDbErr</td>
<td>The number of errors removing a suspect binding record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrCreateAltKeyDbErr</td>
<td>The number of errors creating an alternate key record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrRemoveAltKeyDbErr</td>
<td>The number of errors removing an alternate key record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrFindBindDbErr</td>
<td>The number of errors when encountered for finding a binding record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrEarlyTooLongSrRemoved</td>
<td>The number of sessionRefs found to be in the EarlyMaster or EarlySlave state for too long</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSlavePollingFail</td>
<td>The number of binding capable session initiation requests that were not routed due to polling failures</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSuspectSrRemoved</td>
<td>The number of binding sessionRefs removed as a result of the Suspect Binding mechanism</td>
<td>5 min</td>
</tr>
</tbody>
</table>
**PsbrCreateBindDbErr**

- **Measurement Group:** pSBR Binding Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors creating a binding record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in creating a binding record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrUpdateBindDbErr**

- **Measurement Group:** pSBR Binding Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors updating a binding record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in updating a binding record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrRemoveBindDbErr**

- **Measurement Group:** pSBR Binding Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors removing a suspect binding record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in removing a suspect binding record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.
PsbrCreateAltKeyDbErr

- **Measurement Group:** pSBR Binding Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors creating an alternate key record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in creating an alternate key record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

PsbrRemoveAltKeyDbErr

- **Measurement Group:** pSBR Binding Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors removing an alternate key record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in removing an alternate key record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

PsbrFindBindDbErr

- **Measurement Group:** pSBR Binding Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors when encountered for finding a binding record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in finding a binding record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.
PsbrEarlyTooLongSrRemoved

**Event Group:** pSBR Binding Exception  
**Description:** A count of the number of sessionRefs found to be in the EarlyMaster or EarlySlave state for longer than the Maximum Early Binding Lifetime.  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Collection Interval** 5 min  
**Peg Condition:** Each time sessionRef is discovered that has been in an early state (i.e. EarlyMaster or EarlySlave) for longer than the Maximum Early Binding Lifetime and the following conditions are true:

- PCRF Pooling is Enabled AND
- A binding capable session initiation request is received that matches an existing binding and the binding has been in the EarlyMaster state for longer than the Maximum Early Binding Lifetime OR
- A binding capable session initiation request is received and no slots are available for new sessionRefs, but at least one sessionRef has been in the EarlySlave state for longer than the Maximum Early Binding Lifetime OR
- A slave session polls a master sessionRef that has been in the EarlyMaster state for longer than the Maximum Early Binding Lifetime

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**

1. This measurement gives an indication of the frequency at which binding sessionRefs are discovered in an early state for longer than expected. This unexpected condition could occur if the Maximum Early Binding Lifetime value is configured to be nearly equal to or shorter than the Diameter transaction timer. It could also occur if the binding pSBR was in congestion and load shedding prevented the session from being transitioned from the early state to a final state. In either case the "stuck" sessionRef is removed, preventing it from disrupting further signaling.

2. Contact *My Oracle Support (MOS).*

PsbrSlavePollingFail

**Event Group:** pSBR Binding Exception  
**Description:** A count of the number of binding capable session initiation requests that were not routed to polling failures. This includes the following: slave sessionRef not found, master sessionRef found, but existed for longer than the Maximum Early Binding Lifetime.

**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Collection Interval** 5 min  
**Peg Condition:** Each time an Early Binding Slave session polls the Early Binding master and the following conditions are met:
PCRF Pooling is Enabled AND
- The Early Binding Master sessionRef no longer exists in the binding database OR
- The Early Binding Slave sessionRef no longer exists in the binding database OR
- The Early Binding Master sessionRef exists in the binding database in the EarlyMaster state, but has been in existence for longer than the Maximum Early Binding Lifetime

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**
1. This measurement gives an indication of the Early Binding Slave sessions whose polling attempts did NOT result in a final binding to route towards. Each time this measurement is pegged, P-DRA generates an error answer message using the Binding Found But Unable To Route Diameter result code. The Error-Message AVP contains a 3-digit code that indicates the specific reason for the failure.
2. Contact *My Oracle Support (MOS).*

**PsbrSuspectSrRemoved**

**Measurement Group:** pSBR Binding Exception

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** A count of the number of binding sessionRefs removed as a result of the Suspect Binding mechanism.

**Collection Interval** 5 min

**Peg Condition:** Each time a binding sessionRef is removed by the suspect binding mechanism (i.e. due to inaccessibility of a PCRF for more than 30 seconds while signaling attempts are being performed).

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association

**Recovery:**
1. This measurement gives an indication of the number of binding sessionRefs that were automatically removed from the Policy DRA binding database as a result of continued inability to route binding capable session initiation requests to a given PCRF.
2. Contact *My Oracle Support (MOS).*

**pSBR Session Exception measurements**

The pSBR Session Exception measurement report contains measurements that provide performance information that is specific to the pSBR Session Database.

**Table 77: pSBR Session Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrCreateSessDbErr</td>
<td>The number of errors creating a session record.</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>PsbrRefreshSessDbErr</td>
<td>The number of errors refreshing a session record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrRemSessDbErr</td>
<td>The number of errors terminating a session record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrFindSessionDbErr</td>
<td>The number of errors when encountered for finding a session record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrRemSessRarAttempts</td>
<td>The number of sessions removed as a result of no response being received in 8 consecutive attempts to query the policy client for existence of the session.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**PsbrCreateSessDbErr**

- **Measurement Group:** pSBR Session Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors creating a session record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in creating a session record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrRefreshSessDbErr**

- **Measurement Group:** pSBR Session Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of errors refreshing a session record.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever there is an error in refreshing a session record.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrRemSessDbErr**

- **Measurement Group:** pSBR Session Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of errors terminating a session record.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever there is an error in terminating a session record.
Measurement Scope: All
Recovery: No action necessary.

PsbrFindSessDbErr
Measurement Group: pSBR Session Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of errors when encountered for finding a session record.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever there is an error in finding a session record.
Measurement Scope: All
Recovery: No action necessary.

PsbrRemSessRarAttempts
Measurement Group: pSBR Session Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of sessions removed as a result of no response being received in 8 consecutive attempts to query the policy client for existence of the session.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time a session is removed due to lack of response after the maximum number of attempts to query the policy client have been attempted.
Measurement Scope: Network
Recovery:
1. A non-zero value in this field may indicate that a policy client has become inaccessible after creating Diameter sessions on the Policy DRA.
2. If a policy client was purposely removed from service, please disregard this measurement.
pSBR Audit measurements

The pSBR Audit measurement report contains measurements that provide performance information that is specific to the pSBR Binding Database.

**Table 78: pSBR Audit Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrImsiAuditDbErr</td>
<td>The number of ImsiAnchorKey audit failures due to DB errors</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMsisdnAuditDbErr</td>
<td>The number of MsisdnAlternateKey audit failures due to DB error.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv4AuditDbErr</td>
<td>The number of Ipv4AlternateKey audit failures due to DB error.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv6AuditDbErr</td>
<td>The number of Ipv6AlternateKey audit failures due to DB error.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSessionRecsAudited</td>
<td>The number of Session Records audited during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrExpiredSessionsFound</td>
<td>The number of Expired Session Records found by audit during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrImsiRecsAudited</td>
<td>The number of IMSI Anchor Key Records audited during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrStaleSessionRemoved</td>
<td>The number of stale session records that are terminated by audit.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv4RecsAudited</td>
<td>The number of IPv4 Alternate Key Records audited during the reporting interval</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv4RecsRemoved</td>
<td>The number of IPv4 Alternate Key Records removed by audit during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv6RecsAudited</td>
<td>The number of IPv6 Alternate Key Records audited during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSessionAuditDbErr</td>
<td>The number of Session audit failures due to DB error.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrSessionRefAuditDbErr</td>
<td>The number of SessionRef audit failures due to DB errors.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrImsiAuditCaErr</td>
<td>The number of ImsiAnchorKey audit failures due to ComAgent errors</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMsisdnAuditCongErr</td>
<td>The number of MsisdnAlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>PsbrIpv4AuditCaErr</td>
<td>The number of Ipv4AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv6AuditCaErr</td>
<td>The number of Ipv6AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrIpv6RecsRemoved</td>
<td>The number of IPv6 Alternate Key Records removed by audit during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMsisdnRecsAudited</td>
<td>The number of MSISDN Alternate Key Records audited during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMsisdnRecsRemoved</td>
<td>The number of MSISDN Alternate Key Records removed by audit during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrImsiRecsRemoved</td>
<td>The number of IMSI Anchor Key Records removed by audit during the reporting interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrImsiSrRemovedByAudit</td>
<td>The number of IMSI binding sessionRefs removed as a result of the Binding Audit mechanism</td>
<td>5 min</td>
</tr>
<tr>
<td>PsbrMsisdnSrRemovedByAudit</td>
<td>The number of MSISDN binding sessionRefs removed as a result of the Binding Audit mechanism</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**PsbrImsiAuditDbErr**

- **Measurement Group:** pSBR Audit
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of ImsiAnchorKey audit failures due to DB errors
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is updated whenever an ImsiAnchorKey audit fails due to a DB error.
- **Measurement Scope:** All
- **Recovery:**
  - No action necessary.

**PsbrMsisdnAuditDbErr**

- **Measurement Group:** pSBR Audit
- **Measurement Type:** Simple
Measurements

Measurement Dimension: Single
Description: The number of MsidnAlternateKey audit failures due to DB error.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a MsidnAlternateKey audit fails due to DB error.
Measurement Scope: All
Recovery: No action necessary.

PsbrIpv4AuditDbErr
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Ipv4AlternateKey audit failures due to DB error.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a Ipv4AlternateKey audit fails due to a DB error.
Measurement Scope: All
Recovery: No action necessary.

PsbrIpv6AuditDbErr
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Ipv6AlternateKey audit failures due to DB error.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a Ipv6AlternateKey audit fails due to a DB error.
Measurement Scope: All
Recovery: No action necessary.

PsbrSessionRecsAudited
Measurement Group: pSBR Audit
Measurement Type: Simple
**Measurements**

**PsbrExpiredSessionsFound**
- **Measurement Dimension:** Single
- **Description:** The number of Expired Session Records found by audit during the reporting interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is incremented by one each time a Session record is audited and found to be stale.
- **Measurement Scope:** All
- **Recovery:** No action necessary.

**PsbrImsiRecsAudited**
- **Measurement Group:** pSBR Audit
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of IMSI Anchor Key Records audited during the reporting interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This peg is incremented by one each time an ImsiAnchorKey record is audited.
- **Measurement Scope:** All
- **Recovery:** No action necessary.

**PsbrStaleSessionRemoved**
- **Measurement Group:** pSBR Session Performance
- **Measurement Type:** Simple
Measurements

Measurement Dimension: Single
Description: The number of stale session records that are terminated by audit.
Collection Interval: 5 min
Peg Condition: Every time a session record is audited that finds a time out.
Measurement Scope: All
Recovery: No action necessary.

PsbrIpv4RecsAudited
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of IPv4 Alternate Key Records audited during the reporting interval.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time an Ipv4AlternateKey record is audited.
Measurement Scope: All
Recovery: No action necessary.

PsbrIpv4RecsRemoved
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of IPv4 Alternate Key Records removed by audit during the reporting interval.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time an Ipv4AlternateKey record is removed by audit.
Measurement Scope: All
Recovery: No action necessary.

PsbrIpv6RecsAudited
Measurement Group: pSBR Audit
**PsbrSessionAuditDbErr**

- **Measurement Group**: pSBR Audit
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: The number of Session audit failures due to DB error.
- **Collection Interval**: 5 min
- **Peg Condition**: This peg is updated whenever a Session audit fails due to DB error.
- **Measurement Scope**: All
- **Recovery**: No action necessary.

**PsbrSessionRefAuditDbErr**

- **Measurement Group**: pSBR Audit
- **Measurement Type**: Simple
- **Measurement Dimension**: Single
- **Description**: The number of SessionRef audit failures due to DB errors.
- **Collection Interval**: 5 min
- **Peg Condition**: This peg is updated whenever a SessionRef audit fails due to DB error.
- **Measurement Scope**: All
- **Recovery**: No action necessary.

**PsbrImsiAuditCaErr**

- **Measurement Group**: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of ImsiAnchorKey audit failures due to ComAgent errors
Collection Interval: 5 min
Peg Condition: This peg is updated whenever an ImsiAnchorKey audit fails due to ComAgent error.
Measurement Scope: All
Recovery:
1. Check ComAgent event 19832 - Communication Agent Reliable Transaction Failed and ComAgent measurements CAHSTxDscrCongSR, CAHSTxDscrUnkwnRsrc, and CAHSTxDscrIntErrSR for detailed error causes.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.

PsbrMsisdnAuditCaErr
Measurement Group: pSBR Audit
Measurement Type: Simple
Description: The number of MsidnAlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.
Collection Interval: 5 min
Peg Condition: This peg is updated when a MsidnAlternateKey audit fails due to a ComAgent error.
Measurement Scope: All
Recovery:
1. Check ComAgent event 19832 - Communication Agent Reliable Transaction Failed and ComAgent measurements CAHSTxDscrCongSR, CAHSTxDscrUnkwnRsrc, and CAHSTxDscrIntErrSR for detailed error causes.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.

PsbrIpv4AuditCongErr
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Ipv4AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a Ipv4AlternateKey audit fails due to ComAgent error.
Measurement Scope: All
Recovery:
1. Check ComAgent event 19832 - Communication Agent Reliable Transaction Failed and ComAgent measurements CAHSTxDscrdCongSR, CAHSTxDscrdUnkwnRsrc, and CAHSTxDscrdIntErrSR for detailed error causes.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.

PsbrIpv6AuditCongErr

Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of Ipv6AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.
Collection Interval: 5 min
Peg Condition: This peg is updated whenever a Ipv6AlternateKey audit fails due to ComAgent error.
Measurement Scope: All
Recovery:
1. Refer to ComAgent event 19832 - Communication Agent Reliable Transaction Failed and ComAgent measurements CAHSTxDscrdCongSR, CAHSTxDscrdUnkwnRsrc, and CAHSTxDscrdIntErrSR for detailed error causes.
2. If the problem persists, contact My Oracle Support (MOS) for assistance.

PsbrIpv6RecsRemoved

Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of IPv6 Alternate Key Records removed by audit during the reporting interval.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time an Ipv6AlternateKey record is removed by audit.
Measurement Scope: All
Recovery: No action necessary.

PsbrMsisdnRecsAudited

Measurement Group: pSBR Audit
Measurement Type: Simple
Measurements

Measurement Dimension: Single
Description: The number of MSISDN Alternate Key Records audited during the reporting interval.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time an MsisdnAlternateKey record is audited.
Measurement Scope: All
Recovery: No action necessary.

PsbrMsisdnRecsRemoved
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of MSISDN Alternate Key Records removed by audit during the reporting interval.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time an MsisdnAlternateKey record is removed by audit.
Measurement Scope: All
Recovery: No action necessary.

PsbrImsiRecsRemoved
Measurement Group: pSBR Audit
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of IMSI Anchor Key Records removed by audit during the reporting interval.
Collection Interval: 5 min
Peg Condition: This peg is incremented by one each time an ImsiAnchorKey record is removed by audit.
Measurement Scope: All
Recovery: No action necessary.
PsbrImsiSrRemovedByAudit

**Event Group:** pSBR Audit  
**Description:** A count of the number of IMSI binding sessionRefs removed by the binding audit.  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Collection Interval** 5 min  
**Peg Condition:** Each time the binding audit decides to remove an IMSI binding sessionRef due the following conditions:
- PCRF Pooling is Enabled AND
- The binding sessionRef has been in the database for at least 30 seconds AND
- The binding sessionRef has no corresponding session in the session database

**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association  
**Recovery:**
1. This measurement gives an indication of the number of IMSI bindings that for some reason were not removed when the associated Diameter session either failed or was terminated via signaling. This unexpected condition could occur if binding pSBR congestion load shedding prevented removal of the sessionRef from the binding record.  
2. Contact *My Oracle Support (MOS).*

PsbrMsisdnSrRemovedByAudit

**Measurement Group:** pSBR Audit  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** A count of the number of MSISDN binding sessionRefs removed by the binding audit.  
**Collection Interval** 5 min  
**Peg Condition:** Each time the binding audit decides to remove an MSISDN sessionRef because the binding sessionRef has no corresponding session in the session database.  
**Measurement Scope:** Network Element, Server Group, Resource Domain, Place, Place Association  
**Recovery:**
1. This measurement gives an indication of the number of MSISDN bindings that for some reason were not removed when the associated Diameter session either failed or was terminated via signaling. This unexpected condition could occur if binding pSBR congestion load shedding prevented removal of the sessionRef from the binding record.  
2. Contact *My Oracle Support (MOS).*
Peer Node Performance measurements

The “Peer Node” measurement group is a set of measurements that provide performance information that is specific to a Peer Node. These measurements will allow you to determine how many messages are successfully forwarded and received to/from each Peer Node. Measurements such as the following are included in this group.

Table 79: Peer Routing Rules Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxPeerAnswers</td>
<td>Number of routable Answer messages received from Peer-X</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPeerRequests</td>
<td>Number of routable Request messages received from Peer-X</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPeerAnswers</td>
<td>Number of routable Answer messages sent to Peer-X</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPeerRequests</td>
<td>Number of routable Request messages sent to Peer-X</td>
<td>5 min</td>
</tr>
</tbody>
</table>

RxPeerAnswers

**Measurement Group:** Peer Node Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Peer Node ID)  
**Description:** Number of routable Answer messages received from Peer-X.  
**Collection Interval:** 5 min  
**Peg Condition:** When DRL receives an Answer message event from DCL with a valid Transport Connection ID owned by Peer-X.  
**Measurement Scope:** Server Group  
**Recovery:** No action required.

RxPeerRequests

**Measurement Group:** Peer Node Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Peer Node ID)  
**Description:** Number of routable Request messages received from Peer-X.
Collection Interval: 5 min

Peg Condition: When DRL receives an Request message event from DCL with a valid Transport Connection ID owned by Peer-X.

Measurement Scope: Server Group

Recovery: No action required.

TxPeerAnswers

Measurement Group: Peer Node Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Peer Node ID)

Description: Number of routable Answer messages sent to Peer-X.

Collection Interval: 5 min

Peg Condition: When DRL successfully queues a Request message for Peer-X to DCL.

Measurement Scope: Server Group

Recovery: No action required.

TxPeerRequests

Measurement Group: Peer Node Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Peer Node ID)

Description: Number of routable Request messages sent to Peer-X.

Collection Interval: 5 min

Peg Condition: When DRL successfully queues a Request message for Peer-X to DCL.

Measurement Scope: Server Group

Recovery: No action required.

Peer Routing Rules measurements

The Peer Routing Rules measurement report is a set of measurements associated with the usage of Peer Routing Rules. These measurements allow you to determine which Peer Routing Rules are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed using the Route List.
Table 80: Peer Routing Rules Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxPrtSelected</td>
<td>Number of times that a peer routing rule from PRT-X was selected for routing a Request message.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRuleDuplicatePriority</td>
<td>Number of times that the Peer Routing Rule was selected for routing a message but another Peer Routing Rule had the same priority and was ignored.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRuleFwdFailActionSendAns</td>
<td>Number of times that the Peer Routing Rule was selected for routing a Request message and the message was not successfully routed because the Peer Routing Rule’s Action is “Send Answer”.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRuleFwdFailAll</td>
<td>Number of times that the Peer Routing Rule was selected for routing a Request message and the message was not successfully routed for any reason.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRuleSelected</td>
<td>Number of times that the Peer Routing Rule was selected for routing a Request message.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxMsgPrtMarkedForCpy</td>
<td>Number of Request Messages set to a valid MCCS and marked for Message Copy</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**RxPrtSelected**

**Measurement Group:** Peer Routing Rules  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (PRT ID)  
**Description:** Number of times that a peer routing rule from PRT-X was selected for routing a Request message.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DRL selects a peer routing rule from PRT-X for routing a message.  
**Measurement Scope:** Site  
**Recovery:**  
No action required.
RxRuleDuplicatePriority

Measurement Group: Peer Routing Rules
Measurement Type: Simple
Measurement Dimension: Arrayed (by Peer Routing Rule ID)
Description: The number of times that the Peer Routing Rule was selected for routing a message but another Peer Routing Rule had the same priority and was ignored.
Collection Interval: 5 min
Peg Condition: When the DSR searches the Peer Routing Rules and finds more than one highest priority Peer Routing Rule with the same priority that matches the search criteria.
The measurement is associated with the Peer Routing Rule that is selected for routing.
Measurement Scope: Server Group
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, contact My Oracle Support (MOS).

RxRuleFwdFailActionSendAns

Measurement Group: Peer Routing Rules
Measurement Type: Simple
Measurement Dimension: Arrayed (by Peer Routing Rule ID)
Description: The number of times that the Peer Routing Rule was selected for routing a Request message and the message was not successfully routed because the Peer Routing Rule's action is Send Answer.
Collection Interval: 5 min
Peg Condition: When the DSR selects a Peer Routing Rule to route a Request message and the Peer Routing Rule's action is Send Answer.
Measurement Scope: Server Group
Recovery:
No action required.

RxRuleFwdFailAll

Measurement Group: Peer Routing Rules
Measurement Type: Simple
Measurement Dimension: Arrayed (by Peer Routing Rule ID)
Description: The number of times that the Peer Routing Rule was selected for routing a Request message and the message was not successfully routed for any reason.
Collection Interval: 5 min
Peg Condition: When the DSR selects a Peer Routing Rule to route a Request message and one of the following conditions are met:

1. The Peer Routing Rule's action is Send Answer.
2. The Route List associated with the Peer Routing Rule has an Operational Status of Unavailable.
3. The DSR attempts to route the call but exhausts all routes associated with the Route List and sends an Answer response 3002 (DIAMETER_UNABLE_TO_DELIVER).

The Route List measurement is associated with the Route List selected for routing.

Measurement Scope: Server Group
Recovery:

1. If a Peer Routing Rule has been configured with the action Send Answer, then every time this Peer Routing Rule is selected for routing a message, this measurement will be incremented. A Peer Routing Rule's action can be viewed using the Diameter > Configuration > Peer Routing Rules page.
2. If a Peer Routing Rule has been configured with the action Route to Peer, then every time this Peer Routing Rule is selected for routing a message, the Route List associated with this Peer Routing Rule will be used for routing the message. The Peer Routing Rule's Route List can be viewed using the Diameter > Configuration > Peer Routing Rules page.

RxRuleSelected

Measurement Group: Peer Routing Rules
Measurement Type: Simple
Measurement Dimension: Arrayed (by Peer Routing Rule ID)
Description: The number of times that the Peer Routing Rule was selected for routing a Request message.
Collection Interval: 5 min
Peg Condition: When the DSR selects a Peer Routing Rule for routing a message.
Measurement Scope: Server Group
Recovery:
No action required.

**TxMsgPrtMarkedForCpy**

**Measurement Group:** Peer Routing Rules  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Peer Routing Rule ID)  
**Description:** The number of Request messages set to priority "2" as a result of PRT processing  
**Collection Interval:** 5 min

**Peg Condition:** Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to "Route to Peer" and a Message Priority of "2" is assigned to the peer routing rule.

**Recovery:**  
No action required.

---

**Route List measurements**

The Route List measurement report is a set of measurements associated with the usage of Route Lists. These measurements will allow the user to determine which Route Lists are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed using the Route List.

**Table 81: Route List Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRouteListFailure</td>
<td>Number of times that a Route List was selected for routing a Request message and the DSR was unable to successfully route the message.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRouteListSelected</td>
<td>Number of times the Route List was selected for routing a Request message.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRouteListUnavailable</td>
<td>Number of Request messages from a downstream peer that were rejected by a Local Node because the Route List selected had an &quot;Operational Status&quot; of &quot;Unavailable&quot;.</td>
<td>5 min</td>
</tr>
<tr>
<td>TmRouteListOutage</td>
<td>Time duration that the Route List was unavailable during the measurement interval.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
RxRouteListFailure

**Measurement Group:** Route List  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Route List ID)  
**Description:** The number of times that a Route List was selected for routing a Request message and the DSR was unable to successfully route the message. There are several reasons why a message cannot be routed using a Route List:
- The Operational Status of the Route List is Unavailable
- The peers in the active Route Group do not support the Application ID in the Request message
- The Answer response timer is expiring for messages routed through the active Route Group
- Message loop detection is being detected for the peers in the active Route Group

**Collection Interval:** 5 min  
**Peg Condition:** When the DSR selects a Route List to route a Request message and either the Route List's Operational Status is Unavailable or the DSR attempts to route the call but exhausts all routes associated with the Route List and sends an Answer response 3002 (DIAMETER_UNABLE_TO_DELIVER).

The Route List measurement is associated with the Route List selected for routing.

**Measurement Scope:** Server Group  
**Recovery:**
1. Check the Route List settings using the Diameter > Configuration > Route Lists page.  
2. Contact My Oracle Support (MOS) for assistance if needed.

RxRouteListSelected

**Measurement Group:** Route List  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Route List ID)  
**Description:** Number of times that Route List was selected for routing a Request message.  
**Collection Interval:** 5 min  
**Peg Condition:** When the DSR selects a Route List for routing a message.

The Route List measurement is associated with the Route List selected for routing.

**Measurement Scope:** Server Group  
**Recovery:**  
- No action required.
**RxRouteListUnavailable**

**Measurement Group:** Route List  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Route List ID)  
**Description:** The number of Request messages from a downstream peer that were rejected by a Local Node because the selected Route List had an Operational Status of Unavailable.  
**Collection Interval:** 5 min  
**Peg Condition:** Request message from a downstream peer is rejected by a Local Node because the selected Route List had an Operational Status of Unavailable. This occurs when the Route List was selected via a Peer Routing Rule or implicit routing but its Operational Status was Unavailable.  
The Route List measurement is associated with the Route List selected for routing.  
**Measurement Scope:** Server Group  
**Recovery:**  
1. The operation status of the Route List should be verified using the Diameter > Maintenance > Route Lists page.  
2. Contact *My Oracle Support (MOS)* for assistance if needed.

**TmRouteListOutage**

**Measurement Group:** Route List  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Route List ID)  
**Description:** Time (in seconds) that the Route List was unavailable. This will appear as an aggregate value retrieved from all DA-MPs in a Network Element.  
**Collection Interval:** 5 min  
**Peg Condition:** The time duration interval starts when one of the following conditions occurs:  
1. A new collection interval for the measurement begins and Alarm 22053 - Route List Unavailable is asserted.  
2. Alarm 22053 - Route List Unavailable is asserted.  
The time duration interval stops when one of the following conditions occurs:  
1. The current collection interval for the measurement ends and Alarm 22053 - Route List Unavailable is asserted.  
2. Alarm 22053 - Route List Unavailable is cleared.  
When a time duration interval completes, the time measured is added to the total measurement value.  
**Measurement Scope:** Server Group  
**Recovery:**
1. The operation status of the Route List should be verified using the Diameter > Maintenance > Route Lists page.
2. Contact My Oracle Support (MOS) for assistance if needed.

Routing Usage measurements

The Routing Usage measurement report allows you to evaluate how ingress Request messages are being routed internally within the Relay Agent.

Table 82: Routing Usage Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRoutedIntraMPAttempt</td>
<td>Number of attempts to route an ingress request message via intra-MP routing.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRoutedPeerDirect</td>
<td>Number of Request messages implicitly routed directly to a peer.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRoutedPeerRouteList</td>
<td>Number of Request messages implicitly routed to a peer via its alternate implicit route.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRoutedPrt</td>
<td>Number of Request messages routed using Peer Routing Rules.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

RxRoutedIntraMPAttempt

**Measurement Group:** Routing Usage

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (by Connection ID)

**Description:** The number of attempts to route an ingress request message via intra-MP routing.

**Collection Interval:** 5 min

**Peg Condition:** When the DSR selects a transport connection controlled by the local MP and successfully queues the Request message on the local message queue.

The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

No action required.
**RxRoutedPeerDirect**

- **Measurement Group:** Routing Usage
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** The number of Request messages implicitly routed directly to a peer.
- **Collection Interval:** 5 min
- **Peg Condition:** When the DSR does not find a Peer Routing Rule that matches message content, the Destination-Host AVP is present and its value matches a FQDN of a peer, and the peer is available for egress routing.

The connection measurement is associated with the connection from which the Request message was received.

- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**RxRoutedPeerRouteList**

- **Measurement Group:** Routing Usage
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** The number of Request messages implicitly routed to a peer via its alternate implicit route.
- **Collection Interval:** 5 min
- **Peg Condition:** When the DSR does not find a Peer Routing Rule that matches message content, the Destination-Host AVP is present and its value matches a FQDN of a peer, the peer is Unavailable for egress routing, and the user-defined alternate implicit route for the peer contains a valid Route List.

The connection measurement is associated with the connection from which the Request message was received.

- **Measurement Scope:** Server Group
- **Recovery:** No action required.

**RxRoutedPrt**

- **Measurement Group:** Routing Usage
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
Measurements

**Description:** The number of Request messages routed using Peer Routing Rules.

**Collection Interval:** 5 min

**Peg Condition:** When the DSR selects the highest priority Peer Routing Rule which matches message content.

The connection measurement is associated with the connection from which the Request message was received.

**Measurement Scope:** Server Group

**Recovery:**

No action required.

### Server Exception measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvError</td>
<td>Number of normal errors encountered</td>
<td>30 min</td>
</tr>
<tr>
<td>EvVital</td>
<td>Number of severe errors encountered</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**EvError**

**Measurement Group:** Server Exception

**Measurement Type:** Simple

**Description:** The number of error trace conditions. This indicates that an expected but abnormal path was taken in the software, which warrants further investigation.

By default, error tracing is disabled. Non-zero values in this measurement indicate that something is occurring that would have generated an error trace, were error tracing enabled. These error trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

Contact *My Oracle Support (MOS)* for assistance if any unexpected non-zero values in this measurement occur.

**EvVital**

**Measurement Group:** Server Exception

**Measurement Type:** Simple
**Description:** The number of vital trace conditions encountered. A vital trace indicates that an unexpected path was taken in the software, which warrants further investigation. These vital trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

During application start-up and shutdown, vital traces are used to show details that can aid in debugging of initialization and shutdown problems. These traces are always enabled and cannot be turned off.

It is a VITAL error condition for any other instance.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**
Contact *My Oracle Support (MOS)* for assistance if any unexpected non-zero values in this measurement occur.

### Server TCAP Exception measurements

**Table 83: Server TCAP Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCAPComponentTblFull</td>
<td>Egress operation discarded due to TcapComponent table full.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPRejTcuErr</td>
<td>Operations rejected by TCAP due to TC User error (L-Reject Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPRejPeerErr</td>
<td>Operations rejected by TCAP due to remote TCAP peer error (not counting timeouts – L-Reject Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPRejTcu</td>
<td>Operations rejected by TC User (U-Reject Req).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPRejPeer</td>
<td>Operations rejected by peer (R-Reject Ind + U-Reject Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPRetErrTcu</td>
<td>Operations that caused return error response to peer (U-Error Req).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPRetErrPeer</td>
<td>Operations that received return error response from peer (U-Error Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPOpTimeout</td>
<td>Operations that timed out (invocation timer expiry – egress only L-Cancel Ind).</td>
<td>30 min</td>
</tr>
</tbody>
</table>
### TCAPDialogueTimeout

**Measurement Group:** Server TCAP Exception  
**Measurement Type:** Simple  
**Description:** The number of dialogues aborted by the local TCAP due to a dialogue timeout during the reporting interval.  
**Note:** A dialogue timer is only started if the local TCAP application sends a Begin message that contains no components. The purpose of the dialogue timer is to prevent stale dialogues if the message never reaches the remote TCAP peer or if the remote TCAP peer never responds.  
**Collection Interval:** 30 min  
**Measurement Scope:** Network, NE, Server  

**Recovery:**  
1. If this measurement has a non-zero value, look for Event 19267 in the Alarm History during the time period covered by the measurement reporting interval.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCAPOpCancelTcu</td>
<td>Operations cancelled by TC User (U-Cancel Req).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPStackQueueFull</td>
<td>Stack event discarded due to TCAP task queue full.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPDialogueTblFull</td>
<td>Dialogue discarded due to TcapDialogue table full.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPAbrtTcuErr</td>
<td>Dialogues aborted by TCAP due to TC User error (not counting timeouts – P-Abort Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPAbrtPeerErr</td>
<td>Dialogues aborted by TCAP due to remote TCAP peer error (P-Abort Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPAbrtTcu</td>
<td>Dialogues aborted by TC User (U-Abort Req).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPAbrtPeer</td>
<td>Dialogues aborted by peer (U-Abort Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPDialogueTimeout</td>
<td>Dialogues that timed out (dialogue cleanup timer expiry).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPComponentQueueFull</td>
<td>Operations discarded due to full QueuedComponent array.</td>
<td>30 min</td>
</tr>
<tr>
<td>Ss7DeserializationFail</td>
<td>Number of MAP response message of which deserialization failed.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
2. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPAbrtPeer

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of dialogues aborted by the remote TCAP application using U-Abort during the reporting interval.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
1. If this measurement has a non-zero value, look for Event 19269 in the GUI under Alarm History during the time period covered by the measurement reporting interval.
2. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPAbrtTcu

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of dialogues aborted by the local TCAP during the reporting interval due to a decision by the local TCAP application.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
1. Look for related events in the GUI Alarm History log during the time period of the measurement reporting interval.
2. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPAbrtPeerErr

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of dialogues aborted by the remote TCAP application using P-Abort during the reporting interval.
Measurements

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:

1. If this measurement has a non-zero value, look for Event 19264 or Event 19266 in the GUI under Alarm History during the time period covered by the measurement reporting interval.
2. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPAbrtTcuErr

Measurement Group: Server TCAP Exception

Measurement Type: Simple

Description: The number of dialogues aborted by the local TCAP during the reporting interval due to an error caused by the local TCAP application.

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:

1. If this measurement has a non-zero value, look for Event 19263 or Event 19265 in the GUI under Alarm History during the time period covered by the measurement reporting interval.
2. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPDialogueTblFull

Measurement Group: Server TCAP Exception

Measurement Type: Simple

Description: The number of dialogues (both ingress and egress) discarded during the reporting interval due to the MP server’s internal TCAP dialogue table being full.

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:

If the TCAP dialogue internal table reaches capacity, Alarm 19272 will be raised with critical severity. Please refer to 19272 - TCAP active dialogue utilization if the alarm is asserted.
TCAPStackQueueFull

**Measurement Group:** Server TCAP Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress events discarded during the reporting interval due to the MP server’s TCAP internal event queue being full. Events could be incoming TCAP messages or N-Notice indications from SCCP.  
**Collection Interval:** 30 min  
**Measurement Scope:** Network, NE, Server  
**Recovery:** If the TCAP internal event queue reaches capacity, **Alarm 19274** will be raised with critical severity. See *TCAPStackQueueFull* if the alarm is asserted.

TCAPOpCancelTcu

**Measurement Group:** Server TCAP Exception  
**Measurement Type:** Simple  
**Description:** The number of egress operations that were cancelled by the local TCAP application during the reporting interval.  
**Collection Interval:** 30 min  
**Measurement Scope:** Network, NE, Server  
**Recovery:**  
1. This measurement does not necessarily indicate an error condition. Look for events that may be related during the period of the measurement reporting interval for more details.  
2. Please contact *My Oracle Support (MOS)* as needed for further assistance.

TCAPOpTimeout

**Measurement Group:** Server TCAP Exception  
**Measurement Type:** Simple  
**Description:** The number of egress operations that timed out waiting for a response from the remote TCAP peer during the reporting interval.  
**Collection Interval:** 30 min  
**Measurement Scope:** Network, NE, Server  
**Recovery:**  
1. If this measurement has a non-zero value, look for Event **19268** in the GUI **Alarm History** during the time period covered by the measurement reporting interval.  
2. This error may be caused by failure to route the message by one of the underlying layers (e.g., SCCP). See **19268 - Operation removed by invocation timer expiry** for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPRetErrPeer

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of egress components that resulted in a Return Error response by the remote TCAP peer during the reporting interval.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
1. If this measurement has a non-zero value, look for Event 19275 in the GUI Alarm History during the time period covered by the measurement reporting interval.
2. This error is likely caused by a malformed message or unexpected message that we sent to the remote TCAP peer. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPRetErrTcu

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of ingress components that resulted in a Return Error response by the local TCAP application during the reporting interval.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
1. Look for events in the GUI Alarm History during the time of the measurement reporting interval for more details related to why the component was discarded.
2. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPRejPeer

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of egress components rejected by the remote TCAP peer during the reporting interval.
Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:

1. If this measurement has a non-zero value, look for Event 19271 in the GUI Alarm History during the time period covered by the measurement reporting interval. This error is likely caused by a malformed message or unexpected message that we sent to the remote TCAP peer.
2. If you can locate the corresponding event, see the appropriate documentation for how to proceed. 
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPRejTcu

Measurement Group: Server TCAP Exception

Measurement Type: Simple

Description: The number of ingress components rejected by the local TCAP application during the reporting interval.

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:

1. Look for events in the GUI Alarm History during the time of the measurement reporting interval for more details related to why the component was discarded.
2. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPRejPeerErr

Measurement Group: Server TCAP Exception

Measurement Type: Simple

Description: The number of ingress components discarded due to a component error caused by the remote TCAP peer during the reporting interval.

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:

1. If this measurement has a non-zero value, look for Event 19262 or Event 19266 in the GUI Alarm History during the time period covered by the measurement reporting interval. This error is likely caused by a malformed message or unexpected message from the remote TCAP peer.
2. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.
TCAPRejTcuErr

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of egress components discarded due to a component error caused by the local TCAP application during the reporting interval.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
1. If this measurement has a non-zero value, look for Event 19265 in the GUI Alarm History during the time period covered by the measurement reporting interval.
2. If you can locate the corresponding event, see the appropriate event documentation for how to proceed.
3. Please contact My Oracle Support (MOS) for further assistance in determining the exact cause of the failure.

TCAPComponentTblFull

Measurement Group: Server TCAP Exception
Measurement Type: Simple
Description: The number of egress operations discarded due to the MP server’s TCAP component internal table being full during the reporting interval.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
If the TCAP component internal table reaches capacity, Alarm 19273 will be raised with critical severity. Please refer to 19273 - TCAP active operation utilization if the alarm is asserted.

Ss7DeserializationFail

Measurement Group: Server TCAP Exception
Measurement Dimension: Single
Measurement Type: Simple
Description: The number of MAP response message of which deserialization failed.
Collection Interval: 30 min
Measurement Scope: Network, NE, Server
Recovery:
Contact My Oracle Support (MOS) for assistance if needed.
Server TCAP Performance measurements

Table 84: Server TCAP Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxTCAPDialogues</td>
<td>Number of ingress dialogues created (Begin Ind).</td>
<td>30 min</td>
</tr>
<tr>
<td>TxTCAPDialogues</td>
<td>Number of egress dialogues created (Begin Req).</td>
<td>30 min</td>
</tr>
<tr>
<td>TxTCAPOperations</td>
<td>Number of egress operations created (Invoke Req).</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPStackQueueAvg</td>
<td>TCAP task queue average depth.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPStackQueuePeak</td>
<td>TCAP task queue maximum depth.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPDialogueTblAvg</td>
<td>TcapDialogue table average size.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPDialogueTblPeak</td>
<td>TcapDialogue table maximum size.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPComponentTblAvg</td>
<td>TcapComponent table average size.</td>
<td>30 min</td>
</tr>
<tr>
<td>TCAPComponentTblPeak</td>
<td>TcapComponent table maximum size.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

RxTCAPDialogues

**Measurement Group:** Server TCAP Performance

**Measurement Type:** Simple

**Description:** The number of ingress dialogues created on the MP server during the reporting interval.

**Collection Interval:** 30 min

**Measurement Scope:** Network, NE, Server

**Recovery:**

This measurement shows the number of ingress dialogues (i.e., dialogues resulting from receipt of an ITU TCAP Begin message) created on the MP server during the reporting interval. RxTCAPDialogues divided by the reporting interval yields the average rate of ingress dialogues for the MP server.

TxTCAPDialogues

**Measurement Group:** Server TCAP Performance
**Measurement Type**: Simple

**Description**: The number of egress dialogues created on the MP server during the reporting interval.

**Collection Interval**: 30 min

**Measurement Scope**: Network, NE, Server

**Recovery**: This measurement shows the number of egress dialogues (i.e., dialogues resulting from sending an ITU TCAP Begin message) created on the MP server during the reporting interval. \( \text{TxCAPDialogues} \) divided by the reporting interval yields the average rate of egress dialogues for the MP server.

**TxTCAPOperations**

**Measurement Group**: Server TCAP Performance

**Measurement Type**: Simple

**Description**: The number of egress operations created on the MP server during the reporting interval.

**Collection Interval**: 30 min

**Measurement Scope**: Network, NE, Server

**Recovery**: This measurement shows the number of egress operations (i.e., TCAP Invokes) created on the MP server during the reporting interval. \( \text{TxCAPOperations} \) divided by the reporting interval yields the average rate of egress operations for the MP server.

**TCAPStackQueueAvg**

**Measurement Group**: Server TCAP Performance

**Measurement Type**: Average

**Description**: The average percent utilization during the reporting interval of the MP server’s TCAP internal queue used to receive messages from the SCCP layer. The number is expressed as a percentage of the maximum size.

**Collection Interval**: 30 min

**Measurement Scope**: Network, NE, Server

**Recovery**: If the TCAP internal queue nears capacity, **Alarm 19274** will be raised with a severity corresponding to how near the queue utilization is to 100%. See **19274 - TCAP stack event queue utilization** if the alarm is asserted.

**TCAPStackQueuePeak**

**Measurement Group**: Server TCAP Performance

**Measurement Type**: Maximum
**Description:** The peak percent utilization during the reporting interval of the MP server’s TCAP internal queue used to receive messages from the SCCP layer. The number is expressed as a percentage of the maximum size.

**Collection Interval:** 30 min

**Measurement Scope:** Network, NE, Server

**Recovery:**
- If the TCAP internal queue nears capacity, **Alarm 19274** will be raised with a severity corresponding to how near the queue utilization is to 100%. See **19274 - TCAP stack event queue utilization** if the alarm is asserted.

---

**TCAPDialogueTblAvg**

**Measurement Group:** Server TCAP Performance

**Measurement Type:** Average

**Description:** The average percent utilization during the reporting interval of the MP server’s TCAP dialogue internal table used to maintain dialogue state. The number is expressed as a percentage of the maximum size.

**Collection Interval:** 30 min

**Measurement Scope:** Network, NE, Server

**Recovery:**
- If the TCAP dialogue internal table nears capacity, **Alarm 19272** will be raised with a severity corresponding to how near the queue utilization is to 100%. See **19272 - TCAP active dialogue utilization** if the alarm is asserted.

---

**TCAPDialogueTblPeak**

**Measurement Group:** Server TCAP Performance

**Measurement Type:** Maximum

**Description:** The peak percent utilization during the reporting interval of the MP server’s TCAP dialogue internal table used to maintain dialogue state. The number is expressed as a percentage of the maximum size.

**Collection Interval:** 30 min

**Measurement Scope:** Network, NE, Server

**Recovery:**
- If the TCAP dialogue internal table nears capacity, **Alarm 19272** will be raised with a severity corresponding to how near the queue utilization is to 100%. See **19272 - TCAP active dialogue utilization** if the alarm is asserted.

---

**TCAPComponentTblAvg**

**Measurement Group:** Server TCAP Performance

---
Measurement Type: Average

Description: The average percent utilization during the reporting interval of the MP server’s TCAP component internal table used to maintain operation state. The number is expressed as a percentage of the maximum size.

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:
If the TCAP component internal table nears capacity, Alarm 19273 will be raised with a severity corresponding to how near the queue utilization is to 100%. See 19273 - TCAP active operation utilization if the alarm is asserted.

TCAPComponentTblPeak

Measurement Group: Server TCAP Performance

Measurement Type: Maximum

Description: The peak percent utilization during the reporting interval of the MP server’s TCAP component internal table used to maintain operation state. The number is expressed as a percentage of the maximum size.

Collection Interval: 30 min

Measurement Scope: Network, NE, Server

Recovery:
If the TCAP component internal table nears capacity, Alarm 19273 will be raised with a severity corresponding to how near the queue utilization is to 100%. See 19273 - TCAP active operation utilization if the alarm is asserted.

Session Binding Repository (SBR) Exception measurements

The "SBR Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events specific to the SBR application. Measurements such as the following are included in this group.

Table 85: SBR Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sbr.TxError</td>
<td>Number of error responses sent during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedCreates</td>
<td>Number of load shed error responses per task indicating load shed create sent during the collection interval</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sbr.TxShedWrites</td>
<td>Number of load shed error responses per task indicating load shed write sent during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedReads</td>
<td>Number of load shed error responses per task indicating load shed read sent during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedAll</td>
<td>Number of load shed error responses per task indicating load shed all sent during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.StackQueueFull</td>
<td>Number of StackEvents discarded due to SBR task queue full condition</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedCreatesTot</td>
<td>Number of load shed error responses for create operations during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedWritesTot</td>
<td>Number of load shed error responses for write operations during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedReadsTot</td>
<td>Number of load shed error responses for read operations during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxShedAllTot</td>
<td>Number of load shed error responses for all operations during the collection interval.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**Sbr.TxError**

**Measurement Group:** SBR Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by return code):
- 0 = Unknown message type  
- 1 = SBDB is full  
- 2 = SBDB returned an error  
- 3 = Session record not found  
- 4 = Required parameter was missing  
- 5 = Request shed due to load  

**Description:** The number of error responses sent during the collection interval.  
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented by one each time the SBR application sends an error response.

**Measurement Scope:** Server Group

**Recovery:**
1. Any counts for this measurement should be investigated.
2. For counts of unknown message type (return code 0), SBDB errors (return code 2) or missing parameters (return code 4), contact *My Oracle Support (MOS)* for assistance.
3. For counts of SBDB is full messages (return code 1), additional capacity may be required. Contact *My Oracle Support (MOS)* for assistance.
4. Counts of missing records (return code 3) occur if a session was removed during audit and then another request was received. To prevent this, increase the **Stale SBDB session binding age** setting found on the **CPA > Configuration > SBR** pane.
5. Any counts of requests shed due to load (return code 5) indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. Also check the **Sbr.TxShed** measurements to see which requests are being shed.

**Sbr.StackQueueFull**

- **Measurement Group:** SBR Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Partition ID)
- **Description:** StackEvents discarded due to the SBR’s task queue being full.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented by one each time the SBR discards a StackEvent due to its task queue being full.

**Measurement Scope:** Server Group

**Measurement Dimension:** Arrayed by subresource

**Recovery:** Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The *Sbr.TxError* measurement will also show counts when this measurement shows counts.

**Sbr.TxShedCreates**

- **Measurement Group:** SBR Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Partition ID)
- **Description:** The number of load shed error responses sent that indicate creation operations shed during the collection interval. Creation operations are shed during minor congestion.
- **Collection Interval:** 5 min
Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.

Measurement Scope: Server Group

Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The Sbr.TxError measurement will also show counts when this measurement shows counts. Another associated measurement, Sbr.RxIngressMsgQueueAvg, shows the average percentage of queue length utilization, which is used to determine congestion.

Sbr.TxShedWrites

Measurement Group: SBR Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Partition ID)
Description: The number of load shed error responses sent that indicate update operations shed during the collection interval. Update operations are shed during major congestion.
Collection Interval: 5 min
Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.
Measurement Scope: Server Group
Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The Sbr.TxError measurement will also show counts when this measurement shows counts. Another associated measurement, Sbr.RxIngressMsgQueueAvg, shows the average percentage of queue length utilization, which is used to determine congestion.

Sbr.TxShedReads

Measurement Group: SBR Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (by Partition ID)
Description: The number of load shed error responses sent that indicate read operations shed during the collection interval. Read operations are shed during critical congestion.
Collection Interval: 5 min
Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.
Measurement Scope: Server Group
Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The Sbr.TxError measurement will also show counts when this
measurement shows counts. Another associated measurement, \textit{Sbr.RxIngressMsgQueueAvg}, shows the average percentage of queue length utilization, which is used to determine congestion.

**Sbr.TxShedAll**

- **Measurement Group:** SBR Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Partition ID)
- **Description:** The number of load shed error responses indicating load shed sent during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented by one each time the SBR transmits a load shed error response.
- **Measurement Scope:** Server Group
- **Recovery:** Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The \textit{Sbr.TxError} measurement will also show counts when this measurement shows counts.

**Sbr.TxShedCreatesTot**

- **Measurement Group:** SBR Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The system wide number of load shed error responses for create operations during the collection interval.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time the SBR transmits a load shed error response for a create operation.
- **Measurement Scope:** Server Group
- **Recovery:** No action required

**Sbr.TxShedWritesTot**

- **Measurement Group:** SBR Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The system wide number of load shed error responses for write operations during the collection interval.
- **Collection Interval:** 5 min
Peg Condition: Each time the SBR transmits a load shed error response for a write operation.
Measurement Scope: Server Group
Recovery: No action required

Sbr.TxShedReadsTot
Measurement Group: SBR Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The system wide number of load shed error responses for read operations during the collection interval.
Collection Interval: 5 min
Peg Condition: Each time the SBR transmits a load shed error response for a read operation.
Measurement Scope: Server Group
Recovery: No action required

Sbr.TxShedAllTot
Measurement Group: SBR Exception
Measurement Type: Simple
Measurement Dimension: Single
Description: The system wide number of load shed error responses for all operations during the collection interval.
Collection Interval: 5 min
Peg Condition: Each time the SBR transmits a load shed error response for any operation.
Measurement Scope: Server Group
Recovery: No action required

Session Binding Repository (SBR) Performance measurements

The “SBR Performance” measurement group contains measurements that provide performance information that is specific to the SBR application. Counts for various expected/normal messages and events are included in this group. Measurements such as the following are included.
Table 86: SBR Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sbr.RxCreate</td>
<td>Number of create requests received during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxUpdate</td>
<td>Number of update requests received during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxRead</td>
<td>Number of read requests received during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxDelete</td>
<td>Number of delete requests received during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxStatus</td>
<td>Number of status requests received during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.TxSuccess</td>
<td>Number of success responses sent during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxReqRatePeak</td>
<td>Maximum number of transactions/second processed by the SBR during the reporting interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxServTimeAvg</td>
<td>Average transaction service time in microseconds during the reporting interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxServTimePeak</td>
<td>Peak transaction service time in microseconds during the reporting interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.EvStaleRecRemoved</td>
<td>Number of stale session binding records cleaned by the audit procedure during the reporting interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.EvCreateUpdateMod</td>
<td>Number of create operations turned into update operations during the reporting interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.EvAvgSessionAge</td>
<td>Average age of all current session bindings</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxReqRateAvg</td>
<td>Average of all message processing rate samples taken during the collection interval</td>
<td>5 min</td>
</tr>
</tbody>
</table>
## Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sbr.EvSchdStaleRec</td>
<td>Expected number of stale session bindings scheduled for deletion</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.EvStaleRecRevived</td>
<td>Number of session bindings older than the mostly age that have their timestamps refreshed to the current time</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.EvMostlyStaleSessPartition</td>
<td>Number of session bindings older than the mostly stale age in each partition</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.EvAvgSessionAgePartition</td>
<td>Average age of session binding of a partition</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxIngressMsgQueuePeak</td>
<td>Peak SBR Ingress Message Queue utilization measured during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Sbr.RxIngressMsgQueueAvg</td>
<td>Average SBR Ingress Message Queue utilization measured during the collection interval</td>
<td>5 min</td>
</tr>
</tbody>
</table>

### Sbr.RxCreate

- **Measurement Group:** SBR Performance  
- **Measurement Type:** Simple  
- **Measurement Dimension:** Single  
- **Description:** The number of create requests received during the collection interval.  
- **Collection Interval:** 5 min  
- **Peg Condition:** This measurement is incremented by one each time the SBR application receives a create request.  
- **Measurement Scope:** Server Group  
- **Recovery:** None required

### Sbr.RxUpdate

- **Measurement Group:** SBR Performance  
- **Measurement Type:** Simple  
- **Measurement Dimension:** Single  
- **Description:** The number of update requests received during the collection interval.  
- **Collection Interval:** 5 min
Measurements

**Peg Condition:** This measurement is incremented by one each time the SBR application receives an update request.

**Measurement Scope:** Server Group

**Recovery:** None required

### Sbr.RxRead

**Measurement Group:** SBR Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of read requests received during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented by one each time the SBR application receives a read request.

**Measurement Scope:** Server Group

**Recovery:** None required

### Sbr.RxDelete

**Measurement Group:** SBR Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of delete requests received during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented by one each time the SBR application receives a delete request.

**Measurement Scope:** Server Group

**Recovery:** None required

### Sbr.RxStatus

**Measurement Group:** SBR Performance

**Measurement Type:** Simple

**Measurement Dimension:** Single

**Description:** The number of status requests received during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented by one each time the SBR application receives a status request.
**Measurements**

**Measurement Scope:** Server Group  
**Recovery:** None required

**Sbr.TxSuccess**
- **Measurement Group:** SBR Performance  
- **Measurement Type:** Simple  
- **Measurement Dimension:** Single  
- **Description:** The number of success responses sent during the collection interval.  
- **Collection Interval:** 5 min  
- **Peg Condition:** This measurement is incremented by one each time the SBR application sends a success response.  
- **Measurement Scope:** Server Group  
- **Recovery:** None required

**Sbr.RxReqRatePeak**
- **Measurement Group:** SBR Performance  
- **Measurement Type:** Max  
- **Measurement Dimension:** Single  
- **Description:** The maximum number of transactions/second processed by the SBR during the reporting interval.  
- **Collection Interval:** 5 min  
- **Peg Condition:** This measurement is maximum number of transactions/second processed by the SBR application during the collection interval.  
- **Measurement Scope:** Server Group  
- **Recovery:** None required

**Sbr.RxServTimeAvg**
- **Measurement Group:** SBR Performance  
- **Measurement Type:** Average  
- **Measurement Dimension:** Single  
- **Description:** The average transaction service time in microseconds during the reporting interval  
- **Collection Interval:** 5 min  
- **Peg Condition:** This measurement is the average transaction service time in microseconds processed by the SBR application.  
- **Measurement Scope:** Server Group
Recovery: None required

**Sbr.RxServTimePeak**

- **Measurement Group:** SBR Performance
- **Measurement Type:** Max
- **Measurement Dimension:** Single
- **Description:** The peak transaction service time in microseconds during the reporting interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is the peak transaction service time in microseconds processed by the SBR application.
- **Measurement Scope:** Server Group
- **Recovery:** None required

**Sbr.EvStaleRecRemoved**

- **Measurement Group:** SBR Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of stale session binding records cleaned by the audit procedure during the reporting interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented by one each time the SBR application removes a stale session binding record during the audit procedure. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.
- **Measurement Scope:** Server Group
- **Recovery:** None required

**Sbr.EvCreateUpdateMod**

- **Measurement Group:** SBR Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** The number of create operations turned into update operations during the reporting interval.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented by one each time the SBR application turns a create operation into an update operation. That is, it finds a pre-existing sessionId.
Measurements

Measurement Scope: Server Group
Recovery: None required

Sbr.EvAvgSessionAge
Measurement Group: SBR Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average age in seconds of all current session bindings.
Collection Interval: 5 min
Peg Condition: This measurement is the average age of all current session bindings processed by the SBR application. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.
Measurement Scope: Server Group
Recovery: None required

Sbr.RxReqRateAvg
Measurement Group: SBR Performance
Measurement Type: Average
Measurement Dimension: Single
Description: The average message processing rate per second.
Collection Interval: 5 min
Peg Condition: The average of all message processing rate samples per second taken during the collection interval.
Measurement Scope: Server Group
Recovery: None required

Sbr.EvSchdStaleRec
Measurement Group: SBR Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The expected number of stale session bindings scheduled for deletion.
Collection Interval: 5 min
Peg Condition: This measurement is the expected number of stale session bindings to be deleted during the next stale session binding record audit. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.
**Sbr.EvStaleRecRevived**

**Measurement Group:** SBR Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of session bindings older than the "mostly age" that have their timestamps refreshed to the current time.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented by one each time a session binding that is older than the "mostly stale" age has its timestamp refreshed to the current time.  
**Measurement Scope:** Server Group  
**Recovery:** None required

**Sbr.EvMostlyStaleSessPartition**

**Measurement Group:** SBR Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Partition ID)  
**Description:** The number of session bindings older than the "mostly stale" age in each partition.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented by one each time a session binding becomes older than the "mostly stale" age. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.  
**Measurement Scope:** Server Group  
**Recovery:** None required

**Sbr.EvAvgSessionAgePartition**

**Measurement Group:** SBR Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (by Partition ID)  
**Description:** The average age in seconds of session binding of a partition.  
**Collection Interval:** 5 min
Peg Condition: This measurement will be computed during each partition’s audit process and updated appropriately. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.

Measurement Scope: Server Group
Recovery: None required

**Sbr.RxIngressMsgQueuePeak**

Measurement Group: SBR Performance
 Measurement Type: Max
 Measurement Dimension: Arrayed (by Partition ID)
 Description: The peak SBR Ingress Message Queue utilization measured during the collection interval
 Collection Interval: 5 min
 Peg Condition: This measurement is the peak ingress message queue utilization by the SBR application.
 Measurement Scope: Server Group
 Recovery: None required

**Sbr.RxIngressMsgQueueAvg**

Measurement Group: SBR Performance
 Measurement Type: Average
 Measurement Dimension: Arrayed (by Partition ID)
 Description: The average SBR Ingress Message Queue utilization in percent measured during the collection interval. This measurement, if it goes above 85% percent, will trigger a congestion alarm.
 Collection Interval: 5 min
 Peg Condition: This measurement is the average ingress message queue utilization in percent by the SBR application.
 Measurement Scope: Server Group
 Recovery: None required

**SS7/Sigtran Measurements**

This section provides information about SS7/Sigtran measurement reports and detailed information about each measurement.
Association Exception measurements

Table 87: Association Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxTrFarEndClose</td>
<td>Number of times the far end closed the SCTP connection.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrManClose</td>
<td>The number of times the Transport was manually closed. This includes manual changes of the transport administrative state that caused the transport to transition from APP-UP to Disabled.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrNoRespClose</td>
<td>The number of times the Transport was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrCnxFail</td>
<td>The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections. The number of times an open attempt on UDP socket in Listen Mode failed on the Transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxTrSendFail</td>
<td>The number of times the SCTP/UDP sends failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxTrRcvFail</td>
<td>The number of times an SCTP receive attempt failed on the transport. Failure to receive message via SCTP might result in a message being discarded.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrSockInitFail</td>
<td>Number of times the socket initialization failed.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxM3uaERROR</td>
<td>The number of times an M3UA ERROR message is received by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.</td>
<td>30 min</td>
</tr>
<tr>
<td>TmSingleTransQueueFull</td>
<td>The number of egress messages that were discarded because the single Transport Writer Queue was full.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvAsnUpAckTO</td>
<td>Number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>association start-up (when the association is in the <strong>Enabled</strong> administrative state).</td>
<td></td>
</tr>
<tr>
<td>RxAsnUnsolDownAck</td>
<td>Number of unsolicited M3UA ASP-DOWN-ACK messages received on the association. Unsolicited ASP-DOWN-ACK messages can be sent by the SG to indicate that the SG cannot process traffic on the association.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxAsnInvalidM3ua</td>
<td>Number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvSctpAdjIPToDwn</td>
<td>Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvSctpTransRej</td>
<td>Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**RxTrFarEndClose**

**Measurement Group:** Association Exception  
**Measurement Type:** Simple  
**Description:** Number of times the far end closed the SCTP connection  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time the far-end of the association closes the association by sending either SHUTDOWN or ABORT.  
**Measurement Scope:** NE, Server  

**Recovery:**

1. If the closing of the association was expected, no further action is necessary, the association will be recovered as soon as the far-end is ready to connect again. If the closing of the association was not expected. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Look in the event history from the GUI main menu under Alarms & Events>View History for Event ID 19224 to determine exactly when the far-end closed the association.
3. Look for other events for the association or MP server in the event history.
4. Verify that IP connectivity still exists between the MP server and the SG.
5. Verify whether the far-end of the association is undergoing maintenance.
6. Contact *My Oracle Support (MOS)* for assistance if needed.
EvTrManClose

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the association was manually closed. This includes manual changes of the association administrative state that cause the association to transition from ASP-UP to either ASP-DOWN or Disabled.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time a manual change is made to the association administrative state from Enabled to Blocked or from Enabled to Disabled, causing the association to transition out of ASP-UP protocol state.

Measurement Scope: NE, Server

Recovery:

1. If the association is known to be under maintenance no further action is necessary. If the association was not known to be under maintenance, you can view the Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.

2. View the event history from the GUI main menu under Alarms & Events>View History and look for Event ID 19228. Event ID 19228 shows the manual association state transitions and contains a time-stamp of when the change occurred.

3. View the security logs from the GUI main menu under Security Logs. You can search the logs using the time-stamp from the event history log to determine which login performed the manual state change on the association.

4. Contact My Oracle Support (MOS) for assistance if needed.

EvTrNoRespClose

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of times the association was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the association or to SCTP heartbeating if enabled.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an established SCTP association is closed by the MP server due to lack of response at the SCTP level from the far-end of the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. If it has a non-zero value, the association has been closed due to the lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the signaling gateway. You can view the Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.

2. Look in the event history from the GUI main menu under Alarms & Events>View History for Event ID 19225.
3. Verify IP connectivity between the MP server and the signaling gateway.
4. Determine if the far-end of the association is congested, possibly causing slow response times on the association.
5. Check the IP network between the MP server and the signaling gateway for excessive retransmissions.
6. Contact *My Oracle Support (MOS)* for assistance if needed.

**EvTrCnxFail**

**Measurement Group:** Association Exception  
**Measurement Type:** Simple

**Description:** The number of times the SCTP connection attempt failed on the association. This includes only unsuccessful attempts to connect to the signaling gateway. It does not include failure of established connections.

**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an SCTP connect attempt fails.

**Measurement Scope:** NE, Server

**Recovery:**
1. This measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the signaling gateway at least once and failed to establish the SCTP connection. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Check the event history log from the GUI main menu under Alarms & Events>View History, looking for Event ID 19222. Event ID 19222 provides details about the cause of the failure.
3. Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address. You can view the Adjacent Servers from the GUI main menu under SS7/Sigtran>Configuration>Adjacent Servers.
4. Verify that the remote port configured for the association correctly identifies the port that the signaling gateway is listening on for SCTP connections. You can view the configured port from the GUI main menu under SS7/Sigtran>Configuration>Associations>Configure.
5. Verify the IP network connectivity between the MP server and the signaling gateway.
6. If the signaling gateway must be configured to connect to the MP server’s IP address and port, verify that the signaling gateway configuration matches the association configuration. You can view association data from the GUI main menu under SS7/Sigtran>Configuration>Associations>Configure.
7. Contact *My Oracle Support (MOS)* for assistance if needed.

**TxTrSendFail**

**Measurement Group:** Association Exception  
**Measurement Type:** Simple

**Description:** The number of times the SCTP Send failed for non-DATA M3UA signaling on the association. The number includes the sending of any non-DATA messages on an established association.
**Measurements**

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time an attempt to send M3UA signaling fails for any reason and the information being sent cannot be mapped to a specific link

**Measurement Scope:** NE, Server

**Recovery:**
1. This measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this association using SCTP has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Look in the GUI main menu under Alarms & Events>View History in the event history log for Event ID 19233. Event ID 19233 provides information on the cause of the failure to send.
3. Verify that the IP network between the MP server and the SG is functioning as expected.
4. Contact My Oracle Support (MOS) for assistance if needed.

**RxTrRcvFail**

**Measurement Group:** Association Exception

**Measurement Type:** Simple

**Description:** The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length.

**Measurement Scope:** NE, Server

**Recovery:**
1. This measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.
2. Look in the event history log from the GUI main menu under Alarms & Events>View History for Event ID 19223. Event ID 19223 gives more information about what caused the failure.
3. Try to bring the sockets back into alignment by manually Disabling and Enabling the association.
4. Contact My Oracle Support (MOS) for assistance if needed.

**EvTrSockInitFail**

**Measurement Group:** Association Exception

**Measurement Type:** Simple

**Description:** The number of times the socket initialization failed. Socket initialization includes configuring the association according to the settings in the GUI under SS7/Sigtran>Configuration>Associations>Configuration Sets.

**Collection Interval:** 30 min
**Peg Condition:** This measurement is incremented by one each time one or more socket options cannot be set according to the settings in the association’s configuration set.

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement should have a zero value. A non-zero value indicates a problem with the association setup prior to attempting to connect the association. If this occurs, look for Event ID 19221 in the GUI under Alarms & Events>View History. Event 19221 provides details about the configuration failure.
2. Contact My Oracle Support (MOS) for further assistance.

**RxAsnM3uaERROR**

**Measurement Group:** Association Exception

**Measurement Type:** Simple

**Description:** The number of M3UA ERROR messages received on the association. An M3UA ERROR message is sent by the far-end to complain about an invalid M3UA message that it received.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time an M3UA ERROR message is received that cannot be mapped to a specific link.

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement will have a value of zero. A non-zero value indicates a problem with M3UA signaling sent by the MP server.
2. Look for Event ID 19235 from the GUI main menu under Alarms & Events>View History. Event ID 19235 provides more information about the receipt of the ERROR message.
3. If the ERROR reason in Event ID 19235 indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. Contact My Oracle Support (MOS) for assistance if needed.

**EvAsnUpAckTO**

**Measurement Group:** Association Exception

**Measurement Type:** Simple

**Description:** The number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during the association start-up (when the association is in the Enabled administrative state).

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time an ASP-UP has been sent and the M3UA State Management ACK Timer expires, but no ASP-UP-ACK has been received for the association.

**Measurement Scope:** NE, Server
Recovery:

1. This measurement should have a zero value. If the value is not zero, the association cannot be brought into the state necessary for M3UA ASPTM traffic because the far-end of the association is not responding by sending an ASP-UP-ACK prior to the timeout defined in the GUI under SS7/Sigtran>Configuration>Options>M3UA. The field that defines the timeout is the State Management ACK Timer.

2. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.

3. Check the event history from the GUI main menu under Alarms & Events>View History, looking for Event ID 19226. Event ID 19226 will show when the timeout occurred.

4. Verify that the far-end of the association on the SG is not undergoing maintenance.

5. Verify that the State Management ACK Timer value is not set too short. This should not occur if the IP network is functioning correctly.

6. Verify that the IP network between the MP server and the SG is performing up to expectations.

7. Contact My Oracle Support (MOS) for assistance if needed.

RxAsnUnsolDownAck

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number of unsolicited M3UA ASP-DOWN-ACK messages received on the association. Unsolicited ASP-DOWN-ACK messages can be sent by the SG to indicate that the SG cannot process traffic on the association.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an unsolicited ASP-DOWN-ACK is received on the association.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. A non-zero value means that the far-end of the association has stopped processing M3UA signaling. You can view Association status from the GUI main menu under SS7/Sigtran>Maintenance>Associations.

2. Check the event history from the GUI main menu under Alarms & Events>View History, looking for Event ID 19227. Event ID 19227 will show exactly when the unsolicited ASP-DOWN-ACK was received.

3. Verify whether the far-end of the association is undergoing maintenance.

4. Contact My Oracle Support (MOS) for assistance if needed.

RxAsnInvalidM3ua

Measurement Group: Association Exception

Measurement Type: Simple

Description: The number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.
Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time an M3UA message is received on the association that is invalid due to any syntactic or semantic reason.

Measurement Scope: NE, Server

Recovery:
1. This measurement should have a zero value. In case of a non-zero value in this measurement, review the event history from the GUI main menu under Alarms & Events>View History, looking for Event 19231.
2. Event 19231 provides details about the reason for rejecting the M3UA message. If the error reason indicates a problem with routing context, verify that the routing context used for the association specified in Event 19231 is configured to match between the ASP and the SG.
3. Contact My Oracle Support (MOS) for assistance if needed.

TmSingleTransQueueFull

Measurement Group: Transport Exception

Measurement Type: Simple

Description: The number of egress messages that were discarded because the single Transport Writer Queue was full.

Collection Interval: 30 min

Peg Condition: Check whether the single peers transmit data queue limit has reached its max limit (1000). If maximum limit is reached or exceeded, then peg the measurement and discard the low priority events.

Measurement Scope: NE, Server

Recovery:
This measurement indicates that the Transport is backed up and messages might be discarded. If the value is above the defined critical threshold, an alarm (19408) is generated. If the problem persists, contact My Oracle Support (MOS).

EvSctpAdjPToDwn

Measurement Group: Transport Exception

Measurement Type: Simple

Description: Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.

Collection Interval: 30 min

Peg Condition: This measurement shall be incremented by one each time:

- Reachibility to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected.

Measurement Scope: NE, Server
Recovery:
If all is well, the measurement will have a zero value. A non-zero value indicates that a path fault to that address was detected.

1. Check the event history log at Main Menu>Alarms & Events> View History; look for event ID 19410. Event ID 19410 provides more details about the actual cause of the failure.
2. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at Main Menu>Transport Manager>Configuration>Adjacent Node.
3. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
4. If the problem persists, contact My Oracle Support (MOS).

EvSctpTransRej
Measurement Group: Transport Exception
Measurement Type: Simple
Description: Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.
Collection Interval: 30 min
Peg Condition: This measurement shall be incremented by one each time:
• The association has been rejected due to IP address validation in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.
Measurement Scope: NE, Server
Recovery:
If all is well, the measurement has a zero value. A non-zero value indicates that an Adjacent Node has attempted to connect to the Peer IP Address at least once, but the connection attempt was rejected because the IP address advertised by the Adjacent Node failed validation.

1. Check the Transport history at Main Menu>Transport Manager>Maintenance.
2. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
3. Verify that the SCTP validation mode is the one that is needed.
4. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at Main Menu>Transport Manager>Configuration>Adjacent Node.
5. Verify that the remote port configured at Main Menu>Transport Manager>Configuration>Transport for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.
6. If the problem persists, contact My Oracle Support (MOS).


Association Performance measurements

Table 88: Association Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxTrOctets</td>
<td>The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxTrOctets</td>
<td>The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCTPAssocQueuePeak</td>
<td>The peak SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCTPAssocQueuePeak</td>
<td>The average SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TxTrOctets**

**Measurement Group:** Transport Performance  
**Measurement Type:** Simple  
**Description:** The number of octets sent on the association. This includes octets for both DATA and non-DATA M3UA signaling. It does not include SCTP, IP, or Ethernet headers.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by the number of octets in the message each time:  
- A DATA/non-DATA message is successfully sent on the transport.  
**Measurement Scope:** NE, Server  
**Recovery:** No action required.

**RxTrOctets**

**Measurement Group:** Transport Performance  
**Measurement Type:** Simple  
**Description:** The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.
Collection Interval: 30 min

Peg Condition: This measurement shall be incremented by the number of octets in the message each time:
- A DATA/non-DATA message is successfully received on the transport.

Measurement Scope: NE, Server

Recovery:
- No action required.

**SCTPAssocQueuePeak**

**Measurement Group:** Association Performance

**Measurement Type:** Max

**Description:** The peak SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 30 min

Peg Condition: Transport's queue is registered as a Stack Resource. The StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.

Measurement Scope: NE, Server

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.
4. Contact My Oracle Support (MOS) for assistance if needed.

**SCTPAssocQueueAvg**

**Measurement Group:** Association Performance

**Measurement Type:** Average

**Description:** The average SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 30 min

Peg Condition: The average of all SCTP Single Association Writer Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:
1. This measurement is a measure of how fast the Transport queue is processed and indicates the average depth of queue over the monitored interval.
2. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
3. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.
4. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.
5. If the problem persists, contact My Oracle Support (MOS).

Association Usage measurements

Table 89: Association Usage Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvTrCnxSuccess</td>
<td>The number of times the SCTP connection was successfully established on the transport. The number of times UDP socket in Listen Mode was opened successfully on the Transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>TmAsnBlkNotDown</td>
<td>Number of seconds during the reporting interval during which the association was in the Blocked administrative state but was not in ASP-DOWN state. When the association is Blocked, the desired protocol state is ASP-DOWN. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxTrOctets</td>
<td>The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

EvTrCnxSuccess

Measurement Group: Transport Usage

Measurement Type: Simple

Description: The number of times the SCTP connection was successfully established on the transport. The number of times the UDP socket in Listen Mode was opened successfully on the Transport.
**Collection Interval:** 30 min

**Peg Condition:** This measurement shall be incremented by one each time:

- The SCTP association reaches the APP-UP protocol state (for example, the connection is successfully established).
  
  The UDP socket in Listen Mode was opened successfully.

**Measurement Scope:** NE, Server

**Recovery:**

If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise, preform the following steps:

1. You can view the transport status can be viewed from the GUI main menu under **Transport Manager>Maintenance>Transport**.
2. Look in the event history from the GUI main menu under **Alarms & Events>View History**. Look for events related to the association or the MP server to determine what might have caused the association to fail.
3. Contact **My Oracle Support (MOS)** for assistance if needed.

**TmAsnBlkNotDown**

**Measurement Group:** Association Usage

**Measurement Type:** Duration

**Description:** The number of seconds during the reporting interval during which the association was in the **Blocked** administrative state but was not in ASP-DOWN state. When the association is **Blocked**, the desired protocol state is ASP-DOWN. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.

**Collection Interval:** 30 min

**Peg Condition:** Time is accumulated for this measurement during the collection interval when all of the following are true:

- The association is in the **Blocked** administrative state.
- The association is not in the ASP-DOWN protocol state.

**Measurement Scope:** NE, Server

**Recovery:**

1. The value of this measurement should be zero. A non-zero value indicates that the association was set to the **Blocked** administrative state, but was not able to reach the desired protocol state due to some problem. You can view the Association status from the GUI main menu under **SS7/Sigtran>Maintenance>Associations**.
2. Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address. You can check the configuration from the GUI main menu under **SS7/Sigtran>Configuration>Adjacent Servers**.
3. Verify that the remote port configured for the association correctly identifies the port that the SG is listening on for SCTP connections. You can check the configuration from the GUI main menu under **SS7/Sigtran>Configuration>Associations>Configure**.
4. Verify the IP network connectivity between the MP server and the SG.
5. If the SG must be configured to connect to the MP server’s IP address and port, verify that the SG configuration matches the association configuration. You can check the configuration from the GUI main menu under SS7/Sigtran>Configuration>Associations>Configure.
6. Contact My Oracle Support (MOS) for assistance if needed.

**TmAsnEnaNotUp**

**Measurement Group:** Association Usage  
**Measurement Type:** Duration  
**Description:** The time that the association was enabled, but not in the ASP-UP state  
**Collection Interval:** 30 min  
**Peg Condition:** Time shall be accumulated for this measurement during the collection interval when all of the following are true:
- the association is in the Enabled administrative state
- the association is not in the ASP-UP protocol state for any reason  
**Measurement Scope:** NE, Server  
**Recovery:**  
No action is required.

**Link Exception measurements**

**Table 90: Link Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvLnkActAckTO</td>
<td>Number of times the link timed out waiting for ASP-ACTIVE-ACK. ASP-ACTIVE-ACK is sent by the SG in response to an ASP-ACTIVE message on the link. The link is not available for M3UA data signaling until ASP-ACTIVE-ACK is received.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxLnkUnsolInactAck</td>
<td>Number of times an unsolicited ASP-INACTIVE-ACK was received on the link. ASP-INACTIVE-ACK may be sent unsolicited by the SG to indicate that the specified link is no longer able to process M3UA data signaling. The MP server will begin attempts to bring the link back into the signaling state</td>
<td>30 min</td>
</tr>
</tbody>
</table>
EvLnkActAckTO

Measurement Group: Link Exception

Measurement Type: Simple

Description: The number of times the link timed out waiting for ASP-ACTIVE-ACK. An ASP-ACTIVE-ACK is sent by the SG in response to an ASP-ACTIVE message on the link. The link is not available for M3UA data signaling until the ASP-ACTIVE-ACK is received.

Collection Interval: 30 min

Peg Condition: This measurement is incremented by one each time:

- An ASP-ACTIVE has been sent for the link and the M3UA State Management ACK timer has expired, but no ASP-ACTIVE-ACK was received for the link.

Measurement Scope: NE, Server

Recovery:

1. This measurement should have a zero value. You can view Link status from the GUI main menu under SS7/Sigtran>Maintenance>Links.
2. Check the event history log from the GUI main menu under Alarms & Events>View History. Look for Event ID 19229, which shows when the ASP-ACTIVE-ACK timeout occurs.
3. Verify that the far-end of the link on the SG is not undergoing maintenance.
4. Verify that the State Management ACK Timer period is not set too short.
5. Verify that the IP network between the MP server and the SG is performing up to expectations.
6. Contact My Oracle Support (MOS) for assistance if needed.
**RxLnkUnsolInactAck**

**Measurement Group:** Link Exception  
**Measurement Type:** Simple  
**Description:** The number of times an unsolicited ASP-INACTIVE-ACK was received on the link. ASP-INACTIVE-ACK may be sent unsolicited by the SG to indicate that the specified link is no longer able to process M3UA data signaling. The MP server will begin attempts to bring the link back into the signaling state matching its administrative state. For example, if the link is Enabled, the MP server will attempt to restore M3UA data signaling on the link by sending an ASP-ACTIVE and waiting for an ASP-ACTIVE-ACK.

**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an unsolicited ASP-INACTIVE-ACK is received on the link.

**Measurement Scope:** NE, Server  
**Recovery:**  
1. This measurement should have a zero value. A non-zero value means that the far-end of the link has stopped processing M3UA data. You can view Link status from the GUI main menu under SS7/Sigtran>Maintenance>Links.  
2. Check the event history log from the GUI main menu under Alarms & Events>View History, looking for Event ID 19230. Event ID 19230 will show when the unsolicited ASP-INACTIVE-ACK was received.  
3. Verify whether the far-end of the link is undergoing maintenance.  
4. Contact My Oracle Support (MOS) for assistance if needed.

**RxLnkM3uaERROR**

**Measurement Group:** Link Exception  
**Measurement Type:** Simple  
**Description:** The number of times an M3UA ERROR message was received for the link. M3UA ERROR message are sent to indicate invalid M3UA signaling.

**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time:  
- An M3UA ERROR message is received and that ERROR message can be attributed to a specific link (i.e., the ERROR message contains a valid routing context, or no routing context is needed).

**Measurement Scope:** NE, Server  
**Recovery:**  
1. This measurement should have a value of zero. A non-zero value indicates a problem with the M3UA signaling sent by the MP server.  
2. Look for Event ID 19235 from the GUI main menu under Alarms & Events>View History. Event ID 19235 provides information on the reason for the receipt of the ERROR message.
3. If the ERROR reason in **Event ID 19235** indicates a problem with routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.

4. Contact **My Oracle Support (MOS)** for assistance if needed.

**RxLnkInvalidM3ua**

**Measurement Group:** Link Exception

**Measurement Type:** Simple

**Description:** The number of invalid M3UA messages received on the link. Invalid M3UA messages are messages that violate the M3UA protocol, but which can be attributed to a specific link (i.e., a valid routing context exists or no routing context is necessary).

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time an invalid M3UA message is received for the link.

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement should have a value of zero. A non-zero value indicates a problem with the M3UA signaling received by the MP server.

2. Look for **Event ID 19231** from the GUI main menu under **Alarms & Events>View History**. **Event ID 19231** provides information on the reason the M3UA message was rejected.

3. If the ERROR reason in **Event ID 19231** indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.

4. Contact **My Oracle Support (MOS)** for assistance if needed.

**Link Performance measurements**

**Note:** ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are not counted in these measurement.

**Table 91: Link Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxLnkMSU</td>
<td>Number of MSUs sent on the link. MSUs includes all M3UA messages, both DATA and non-DATA.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxLnkMSU</td>
<td>Number of MSUs received on the link. MSUs includes all M3UA messages, both DATA and non-DATA.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxLnkMSUOctets</td>
<td>Number of MSU octets sent on the link. MSU octets includes all</td>
<td>30 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>M3UA messages, both DATA and non-DATA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RxLnkMSUOctets</td>
<td>Number of MSU octets received on the link. MSU octets includes all M3UA messages, both DATA and non-DATA.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TxLnkMSU**

**Measurement Group:** Link Performance  
**Measurement Type:** Simple  
**Description:** The number of MSUs sent on the link, including all M3UA messages, both DATA and non-DATA.  
**Note:** ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an M3UA message is sent on the link.  
**Measurement Scope:** NE, Server  
**Recovery:** No action required.

**RxLnkMSU**

**Measurement Group:** Link Performance  
**Measurement Type:** Simple  
**Description:** The number of MSUs received on the link. MSUs includes all M3UA messages, both DATA and non-DATA. Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an M3UA message is received on the link.  
**Measurement Scope:** NE, Server  
**Recovery:** No action required.

**TxLnkMSUOctets**

**Measurement Group:** Link Performance
**RxLnkMSUOctets**

**Measurement Group:** Link Performance

**Measurement Type:** Simple

**Description:** The number of MSU octets received on the link – MSU octets includes all M3UA messages, both DATA and non-DATA. Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by the number of octets in the MSU (not including SCTP, IP, or Ethernet headers) each time an M3UA message is received on the link.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

---

**Link Set Performance measurements**

**Table 92: Link Set Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxLnkSetMSU</td>
<td>Number of MSUs sent on the link set. MSUs includes all M3UA DATA messages sent on all links in the link set.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxLnkSetMSU</td>
<td>Number of MSUs received on the link set. MSUs includes all M3UA DATA messages received on all links in the link set.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxLnkSetMSUOctets</td>
<td>Number of MSU octets sent on the link set. MSU octets includes</td>
<td>30 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>all M3UA DATA octets sent on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.</td>
<td></td>
</tr>
<tr>
<td>RxLnkSetMSUOctets</td>
<td>Number of MSU octets received on the link set. MSU octets includes all M3UA DATA octets received on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TxLnkSetMSU**

- **Measurement Group:** Link Set Performance
- **Measurement Type:** Simple
- **Description:** The number of MSUs sent on the link set, including all M3UA DATA messages sent on all links in the link set.
- **Collection Interval:** 30 min
- **Peg Condition:** This measurement is incremented by one each time an M3UA DATA message is sent on a link in the link set.
- **Measurement Scope:** NE, Server
- **Recovery:** No action required.

**RxLnkSetMSU**

- **Measurement Group:** Link Set Performance
- **Measurement Type:** Simple
- **Description:** The number of MSUs received on the link set. MSUs includes all M3UA DATA messages received on all links in the link set.
- **Collection Interval:** 30 min
- **Peg Condition:** This measurement is incremented by one each time an M3UA DATA message is received on a link in the link set.
- **Measurement Scope:** NE, Server
- **Recovery:** No action required.

**TxLnkSetMSUOctets**

- **Measurement Group:** Link Set Performance
**Measurement Type:** Simple  
**Description:** The number of MSU octets sent on the link set, including all M3UA DATA octets sent on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by the number of octets in the M3UA DATA message each time an M3UA DATA message is sent on a link in the link set.  
**Measurement Scope:** NE, Server  
**Recovery:**  
No action required.

**RxLnkSetMSUOctets**  
**Measurement Group:** Link Set Performance  
**Measurement Type:** Simple  
**Description:** The number of MSU octets received on the link set. MSU octets include all M3UA DATA octets received on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by the number of octets in the M3UA DATA message each time an M3UA DATA message is received on a link in the link set.  
**Measurement Scope:** NE, Server  
**Recovery:**  
No action required.

**Link Set Usage measurements**

**Table 93: Link Set Usage Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TmM3RLLinksetUnavail</td>
<td>Total time (in seconds) that all links in the link set were unavailable to M3RL during the measurement interval, regardless of whether the links were automatically or manually made unavailable.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TmM3RLLinksetUnavail**  
**Measurement Group:** Link Set Usage  
**Measurement Type:** Duration
**Description:** Total time (in seconds) that all links in the link set were unavailable to M3RL during the measurement interval, regardless of whether the links were automatically or manually made unavailable.

**Collection Interval:** 30 min

**Peg Condition:** M3RL must maintain an accurate time and measurement of the number of seconds during the collection period that the Link Set’s state is **Unavailable**. This measurement is associated with the duration (in seconds) that **Alarm 19202 Link Set Unavailable** is asserted during the collection period.

Start of duration measurement for Link Set "X" criteria:

1. **Alarm 19202** is asserted for Link Set "X."
2. Start of new collection period AND **Alarm 19202** for Linkset "X" is already asserted (during a previous collection interval).

Stop of duration measurement for Link Set "X" criteria:

1. **Alarm 19202** for Linkset "X" is cleared (i.e, Link Set becomes **Available**).
2. End of collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

This value provides a measure of the availability of a Link Set. No action required.

### Link Usage measurements

**Table 94: Link Usage Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TmLnkMOOS</td>
<td>Number of seconds the link is manual out of service during the reporting period. A link is manual out of service when the link is in the Disabled administrative state.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
| TmLnkOOS        | Number of seconds the link is out of service for any reason during the reporting period. A link may be out of service due to:  
• Maintenance activity: link is Disabled or the link’s association is Disabled or Blocked.  
• Failure of the link to receive ASP-ACTIVE-ACK. | 30 min              |
**TmLnkMOOS**

**Measurement Group:** Link Usage  
**Measurement Type:** Duration  
**Description:** The number of seconds the link is manual out of service during the reporting period. A link is manual out of service when the link is in the **Disabled** administrative state.  
**Collection Interval:** 30 min  
**Peg Condition:** Time is accumulated for this measurement when the link administrative state is set to **Disabled**.  
**Note:** The link is not considered to be manually out of service if the link is in the **Enabled** administrative state even if the association that hosts the link is manually out of service.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If a non-zero value in this field is unexpected (i.e., no link maintenance is known to have occurred), the link status can be viewed from the GUI under **SS7/Sigtran>Maintenance>Links**.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TmLnkAvailable</td>
<td>Number of seconds the link is in service during the reporting period. The link is considered to be in service if the link’s status reason is <strong>Normal</strong>. An in-service link is available for M3UA DATA signaling.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvLnkManClose</td>
<td>Number of times a link was closed due to manual action. This count indicates the number of times that a link transitioned from ASP-ACTIVE to ASP-INACTIVE as a direct result of someone changing the link administrative state from <strong>Enabled</strong> to <strong>Disabled</strong>.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
2. Also, look in the GUI main menu under Alarms & Events>View History in the event history for Event ID 19234. Event 19234 records each change in the link’s administrative state. If the link was known to be under maintenance, this value represents the number of seconds during the reporting period that the link was in the Disabled administrative state.

TmLnkOOS

Measurement Group: Link Usage  
Measurement Type: Duration  

Description: The number of seconds the link is out of service for any reason during the reporting period. A link may be out of service due to the following conditions:

- Maintenance activity – link is Disabled or link’s association is Disabled or Blocked.
- Failure of the link to receive ASP-ACTIVE-ACK.
- Receipt of unsolicited ASP-INACTIVE-ACK from the SG.
- The link’s association is not in the Normal status – failed to establish SCTP connection, failed to receive ASP-UP-ACK, received unsolicited ASP-DOWN-ACK.

Collection Interval: 30 min

Peg Condition: Time is accumulated for this measurement when the link status reason is not Normal.

Measurement Scope: NE, Server

Recovery:
1. This measurement should have a value of zero. If the link or the link’s association is known to be under maintenance, then a non-zero value in this measurement is expected.
2. Otherwise, the link status can be viewed from the GUI main menu under SS7/Sigtran>Maintenance>Links.
3. Also look in the event history from the GUI main menu under Alarms & Events>View History for events related to this link or the link’s association.
4. Contact My Oracle Support (MOS) for assistance if needed.

TmLnkAvailable

Measurement Group: Link Usage  
Measurement Type: Duration  

Description: The number of seconds the link is in service during the reporting period. The link is considered to be in service if the link’s status reason is Normal. An in-service link is available for M3UA DATA signaling.

Collection Interval: 30 min

Peg Condition: Time is accumulated for this measurement when the link status reason is Normal.

Measurement Scope: NE, Server

Recovery:
1. If all is well, this value should equal the length of the reporting period, meaning that the link was active for the entire reporting period. If the link-available time is not equal to the reporting period, it could be due to one of the following conditions:
• Link maintenance. The measurements \text{TmLnkMOOS} and \text{TmLnkOOS} should have a non-zero values. See the actions for \text{TmLnkMOOS}.
• Link failure. The measurement \text{TmLnkOOS} should have a non-zero value. See the actions for \text{TmLnkOOS}.
• The link was added during the reporting period. The report indicates that the data is incomplete for the reporting period.

2. Contact \textit{My Oracle Support (MOS)} for assistance if needed.

\textbf{EvLnkManClose}

\textbf{Measurement Group}: Link Usage
\textbf{Measurement Type}: Simple

\textbf{Description}: The number of times a link was closed due to manual action. This count indicates the number of times that a link transitioned from ASP-ACTIVE to ASP-INACTIVE as a direct result of someone changing the link administrative state from \textit{Enabled} to \textit{Disabled}.

\textbf{Collection Interval}: 30 min

\textbf{Peg Condition}: This measurement is incremented by one each time:

• The link administrative state is changed from \textit{Enabled} to \textit{Disabled}, causing a protocol state transition from ASP-ACTIVE to ASP-INACTIVE.

\textbf{Measurement Scope}: NE, Server

\textbf{Recovery}:

1. If the link is known to be under maintenance, then no further action is necessary. If the link was not known to be under maintenance, then link status can be viewed from the GUI main menu under SS7/Sigtran>Maintenance>Links.
2. View the event history from the GUI main menu under Alarms & Events>View History looking for Event ID 19234. Event ID 19234 shows the manual link state transitions and contains a time-stamp of when the change occurred.
3. The security logs from the GUI main menu under Security Logs can be searched using the time-stamp from the event history log to determine which login performed the manual state change on the link.
4. Contact \textit{My Oracle Support (MOS)} for assistance if needed.

\textbf{Server M3UA Exception measurements}

\textbf{Table 95: Server M3UA Exception Measurement Report Fields}

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxM3uaERROR</td>
<td>Number of M3UA ERROR messages sent by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some reason.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
## Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>problem with the message syntax or semantics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RxM3uaERROR</td>
<td>Number of times an M3UA ERROR messages received by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.</td>
<td>30 min</td>
</tr>
<tr>
<td>M3UAStackQueueFull</td>
<td>Number of messages that were discarded because the M3UA Stack Event Queue was full</td>
<td>30 min</td>
</tr>
<tr>
<td>SCTPAggrQueueFull</td>
<td>Number of egress messages that were discarded because the maximum number of SCTP messages queued in all SCTP Single Association Writer Queues exceeded a maximum capacity.</td>
<td>30 min</td>
</tr>
<tr>
<td>ANSIDiscardsNoPDUBuffer</td>
<td>ANSI ingress message discarded: no PDU buffer.</td>
<td>30 min</td>
</tr>
<tr>
<td>ITUDiscardsNoPDUBuffer</td>
<td>The number of ingress messages that were discarded because no ITU/ITUN PUD Buffers were available.</td>
<td>30 min</td>
</tr>
<tr>
<td>ItuiRxNoPDUBuffer</td>
<td>ITU Ingress Message Discarded - No PDU Buffer</td>
<td>30 min</td>
</tr>
<tr>
<td>ItunRxNoPDUBuffer</td>
<td>ITUN Ingress Message Discarded - No PDU Buffer</td>
<td>30 min</td>
</tr>
</tbody>
</table>

### TxE3uaERROR

**Measurement Group:** Server M3UA Exception  
**Measurement Type:** Simple  
**Description:** The number of M3UA ERROR messages sent by the MP server. M3UA ERROR message are sent to inform the originator of an M3UA message that the message cannot be processed due to some problem with the message syntax or semantics.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time an ERROR message is sent.  
**Measurement Scope:** NE, Server
Recovery:

1. If all is well this measurement will have a zero value. If this measurement has a non-zero value, review the event history in the GUI under Alarms & Events>View History. Look for Event ID 19231.

   Event ID 19231 provides details about the reason for sending the M3UA ERROR message

2. If the error reason in Event ID 19231 indicates a problem with the routing context, verify that the routing context used for the specified link is configured to match between the ASP and the SG.

3. Contact My Oracle Support (MOS) for assistance if needed.

RxM3uaERROR

Measurement Group: Server M3UA Exception
Measurement Type: Simple
Description: The number of times M3UA ERROR messages are received by the MP server. M3UA ERROR messages are sent to inform the originator of an M3UA message that the message cannot be processed because of a problem with the message syntax or semantics.
Collection Interval: 30 min
Peg Condition: This measurement is incremented by one each time an ERROR message is received.
Measurement Scope: NE, Server
Recovery:

1. This measurement should have a zero value. If the value is non-zero, view the event history from the GUI main menu under Alarms & Events>View History and look for Event ID 19235.

2. Event ID 19235 provides details about the reason for receiving the M3UA ERROR message. If the reason indicates a problem with the routing context, verify that the routing context used for the link specified in Event ID 19235 is configured to match between the ASP and the SG.

3. Contact My Oracle Support (MOS) for assistance if needed.

M3UAStackQueueFull

Measurement Group: Server M3UA Exception
Measurement Type: Simple
Description: The number of messages that were discarded because the M3UA Stack Event Queue was full. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

**SCTPAggrQueueFull**

**Measurement Group:** Server M3UA Exception  
**Measurement Type:** Simple  
**Description:** The number of egress messages that were discarded because the number of SCTP messages queued in all SCTP Single Association Writer Queues exceeded a maximum capacity.  
**Collection Interval:** 30 min  
**Peg Condition:** For each SCTP Aggregate Association Writer Queue message discarded.  
**Measurement Scope:** NE, Server  
**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 GUI main menu under 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 monitor MP server status from Status & Manage>Server.  
4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from Status & Manage>KPIs. Each MP in the server site should be receiving approximately the same ingress transactions 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, contact My Oracle Support (MOS).

**ANSIRxNoPDUBuffer**

**Measurement Group:** Server M3UA Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress ANSI messages that were discarded because no ANSI PDU Buffers were available.  
**Collection Interval:** 30 min  
**Peg Condition:** For each ANSI message discarded  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If this measurement is greater than zero, a network (IP or SS7) problem might exist or an MP-specific software problem may exist (for example, a buffer pool leak).  
2. If the problem persists, contact My Oracle Support (MOS).
**ItuiRxNoPDUBuffer**

**Measurement Group:** Server M3UA Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress ITUI messages that were discarded because no ITUI PDU Buffers were available.  
**Collection Interval:** 30 min  
**Peg Condition:** For each ITUI message discarded  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If this measurement is greater than zero, a network (IP or SS7) problem might exist or an MP-specific software problem might exist (for example, a buffer pool leak).  
2. If the problem persists, contact *My Oracle Support (MOS)*.

**ItunRxNoPDUBuffer**

**Measurement Group:** Server M3UA Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress ITUN messages that were discarded because no ITUN PDU Buffers were available.  
**Collection Interval:** 30 min  
**Peg Condition:** For each ITUN message discarded  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. ITUN PDU is allocated to each ITUN message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues. Under normal circumstances, the PDU Buffer Pool should never be 100% utilized.  
2. If this measurement is greater than zero, then a network (IP or SS7) problem may exist or an MP-specific software problem may exist (e.g., a buffer pool leak).  
3. If the problem persists, contact *My Oracle Support (MOS)*.

### Server M3UA Performance measurements

**Table 96: Server M3UA Performance Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxNonDataMsg</td>
<td>Non-DATA messages sent by the MP server. This includes all</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxNonDataMsg</td>
<td>Non-DATA messages received by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxNonDataOctets</td>
<td>Non-DATA octets sent by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxNonDataOctets</td>
<td>Non-DATA octets received by the MP server. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.</td>
<td>30 min</td>
</tr>
<tr>
<td>M3UAStackQueuePeak</td>
<td>Peak M3UA Network Management Event Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>M3UAStackQueueAvg</td>
<td>Average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCTPAggrQueuePeak</td>
<td>Peak SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCTPAggrQueueAvg</td>
<td>Average of all SCTP Aggregate Association Writer Queue utilization samples taken during the collection interval.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
**TxNonDataMsg**

**Measurement Group:** Server M3UA Performance  
**Measurement Type:** Simple  
**Description:** This measurement gives the level of non-DATA M3UA signaling that occurred on the MP server during the reporting period. The count includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release.  
**Collection Interval:** 30 min, Daily  
**Peg Condition:** This measurement is incremented by one each time any of the following occur:  
- An ASP-UP message is sent.  
- An ASP-DOWN message is sent.  
- An ASP-ACTIVE message is sent.  
- An ASP-INACTIVE message is sent.  
- An ERROR message is sent.  
- A DAUD message is sent.  
- A BEAT message is sent.  
- A BEAT-ACK message is sent.  
**Measurement Scope:** NE, Server  
**Recovery:**  
- No action required.

---

**RxNonDataMsg**

**Measurement Group:** Server M3UA Performance  
**Measurement Type:** Simple  
**Description:** This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time any of the following occur:  
- An ASP-UP-ACK message is received  
- An ASP-DOWN-ACK message is received  
- An ASP-ACTIVE-ACK message is received  
- An ASP-INACTIVE-ACK message is received  
- An ERROR message is received  
- A DUNA message is received  
- A DAVA message is received  
- A DRST message is received  
- A SCON message is received  
- A DUPU message is received  
- A BEAT message is received  
- A BEAT-ACK message is received
• A NOTIFY message is received

**Measurement Scope:** NE, Server

**Recovery:**
No action required.

**TxNonDataOctets**

**Measurement Group:** Server M3UA Performance

**Measurement Type:** Simple

**Description:** This measurement gives the number of octets of non-DATA M3UA signaling that occurred on the MP server during the reporting period. The count includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, ERROR, DAUD). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by the number of octets in the message (not including SCTP, IP, or Ethernet headers) each time any of the following occur:

• An ASP-UP message is sent.
• An ASP-DOWN message is sent.
• An ASP-ACTIVE message is sent.
• An ASP-INACTIVE message is sent.
• An ERROR message is sent.
• A DAUD message is sent.
• A BEAT message is sent.
• A BEAT-ACK message is sent.

**Measurement Scope:** NE, Server

**Recovery:**
No action required.

**RxNonDataOctets**

**Measurement Group:** Server M3UA Performance

**Measurement Type:** Simple

**Description:** This measurement gives the number of octets of non-DATA M3UA signaling occurring on the MP server during the reporting period. This includes all non-DATA M3UA messages (i.e., ASPSM, ASPTM, MGMT, SSNM). RKM messaging is not supported in this release. SCTP, IP, and Ethernet headers are not included in the octet counts.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by the number of octets in the message (not including SCTP, IP, or Ethernet headers) each time any of the following occur:

• An ASP-UP-ACK message is received
• An ASP-DOWN-ACK message is received
An ASP-ACTIVE-ACK message is received
An ASP-INACTIVE-ACK message is received
An ERROR message is received
A DUNA message is received
A DAVA message is received
A DRST message is received
A SCON message is received
A DUPU message is received
A BEAT message is received
A BEAT-ACK message is received
A NOTIFY message is received

Measurement Scope: NE, Server

Recovery:

No action required.

M3UAStackQueuePeak

Measurement Group: Server M3UA Performance

Measurement Type: Max

Description: The peak M3UA Network Management Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The maximum M3UA Stack Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

M3UAStackQueueAvg

Measurement Group: Server M3UA Performance

Measurement Type: Average

Description: The average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min
**Peg Condition:** The average of all M3UA Stack Event Queue utilization samples taken during the collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

3. Contact *My Oracle Support (MOS)* for assistance if needed.

**SCTPAggrQueuePeak**

**Measurement Group:** Server M3UA Performance

**Measurement Type:** Max

**Description:** The peak SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.

**Collection Interval:** 30 min

**Peg Condition:** The maximum SCTP Aggregate Association Writer Queue utilization sample taken during the collection interval.

**Measurement Scope:** NE, Server

**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 the GUI main menu under 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 monitor MP server status from Status & Manage>Server.

4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from Status & Manage>KPIs. Each MP in the server site should be receiving approximately the same ingress transaction per second.

5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from Status & Manage>KPIs. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

6. If the problem persists, contact *My Oracle Support (MOS)*.

**SCTPAggrQueueAvg**

**Measurement Group:** Server M3UA Performance

**Measurement Type:** Average
**Description:** The average SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.

**Collection Interval:** 30 min

**Peg Condition:** The average of all SCTP Aggregate Association Writer Queue utilization samples taken during the collection interval.

**Measurement Scope:** NE, Server

**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 the GUI main menu under 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 monitor MP server status from Status & Manage > Server.

4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from Status & Manage > KPIs. Each MP in the server site should be receiving approximately the same ingress transaction per second.

5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from Status & Manage > KPIs. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

6. If the problem persists, contact My Oracle Support (MOS).

**Server M3UA Usage measurements**

**Table 97: Server M3UA Usage Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxASPSM</td>
<td>Number of ASPSM messages sent by the MP server.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxASPSM</td>
<td>Number of ASPSM messages received by the server.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxASPTM</td>
<td>Number of ASPTM messages sent by the MP server.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxASPTM</td>
<td>Number of ASPTM messages received by the MP server.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxDAUD</td>
<td>Number of DAUD messages sent by the MP server. DAUD message are sent periodically as an audit when the SG reports that a point code is unavailable or congested.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxSSNM</td>
<td>Number of SSNM messages received by the MP server. SSNM messages are sent from the SG as information about point code and user part status in the network.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxM3uaNOTIFY</td>
<td>Number of M3UA NOTIFY messages received by the MP server. M3UA NOTIFY messages are sent by the SG to indicate its view of the M3UA AS state. These messages do not cause any signaling behavior on the MP server.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TxASPSM**

**Measurement Group:** Server M3UA Usage  
**Measurement Type:** Simple  
**Description:** This measurement gives the level of ASPSM M3UA signaling that occurs on the MP server during the reporting period.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time any of the following occur:
- An ASP-UP message is sent.
- An ASP-DOWN message is sent.
- A BEAT message is sent.
- A BEAT-ACK message is sent.  
**Measurement Scope:** NE, Server  
**Recovery:** No action required.

**RxASPSM**

**Measurement Group:** Server M3UA Usage  
**Measurement Type:** Simple  
**Description:** This measurement gives the level of ASPSM M3UA signaling occurring on the MP server during the reporting period.  
**Collection Interval:** 30 min  
**Peg Condition:** This measurement is incremented by one each time any of the following occur:
- An ASP-UP-ACK message is received  
- An ASP-DOWN-ACK message is received
• A BEAT message is received
• A BEAT-ACK message is received
Measurement Scope: NE, Server
Recovery:
No action required.

TxASPTM
Measurement Group: Server M3UA Usage
Measurement Type: Simple
Description: This measurement gives the level of ASPTM M3UA signaling that occurs on the MP server during the reporting period.
Collection Interval: 30 min
Peg Condition: This measurement is incremented by one each time any of the following occur:
• An ASP-ACTIVE message is sent.
• An ASP-INACTIVE message is sent.
Measurement Scope: NE, Server
Recovery:
No action required.

RxASPTM
Measurement Group: Server M3UA Usage
Measurement Type: Simple
Description: This measurement gives the level of ASPTM M3UA signaling occurring on the MP server during the reporting period.
Collection Interval: 30 min
Peg Condition: This measurement is incremented by one each time any of the following occur:
• An ASP-ACTIVE-ACK message is received
• An ASP-INACTIVE-ACK message is received
Measurement Scope: NE, Server
Recovery:
No action required.

TxDAUD
Measurement Group: Server M3UA Usage
Measurement Type: Simple
**Measurements**

**Description:** This measurement indicates the level of auditing that occurs on the MP server during the reporting period. AUD message are sent periodically as an audit when the SG reports that a point code is unavailable or congested.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time a DAUD message is sent.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

**RxBSSNM**

**Measurement Group:** Server M3UA Usage

**Measurement Type:** Simple

**Description:** The number of SSNM messages received by the MP server. SSNM messages are sent from the SG as information about point code and user part status in the network. This measurement indicates the level of SSNM signaling occurring on the MP server during the reporting period.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by the number of octets in the message (not including SCTP, IP, or Ethernet headers) each time any of the following occur:

- A DUNA message is received
- A DAVA message is received
- A DRST message is received
- A SCON message is received
- A DUPU message is received

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

**RxM3uaNOTIFY**

**Measurement Group:** Server M3UA Usage

**Measurement Type:** Simple

**Description:** The number of M3UA NOTIFY messages received by the MP server. M3UA NOTIFY messages are sent by the SG to indicate its view of the M3UA AS state. These messages do not cause any signaling behavior on the MP server.

**Collection Interval:** 30 min

**Peg Condition:** This measurement is incremented by one each time a NOTIFY message is received.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.
## Server MTP3 Exception measurements

Table 98: Server MTP3 Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxM3RLDestUnknown</td>
<td>Number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxM3RLDestUnavail</td>
<td>Number of egress messages M3RL discarded because the RSP/Destination was Unavailable.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxM3RLDestCong</td>
<td>Number of egress messages M3RL discarded because the RSP/Destination’s congestion level was higher than the message’s priority.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxM3RLBufOverflow</td>
<td>Number of egress messages M3RL discarded because of an internal buffer overflow.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxM3RLInvalidDPC</td>
<td>Number of ingress messages M3RL discarded because the DPC was not the True Point Code (TPC) or Capability Point Code (CPC) configured for the MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxM3RLInvalidSI</td>
<td>Number of ingress messages M3RL discarded because the Service Indicator received was not &quot;0&quot; (SNM) or &quot;3&quot; (SCCP).</td>
<td>5 min</td>
</tr>
<tr>
<td>RxM3RLInvalidNI</td>
<td>Number of ingress messages M3RL discarded because the Network Indicator received was not the same value configured for the MP.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxM3RLBufOverflow</td>
<td>Number of ingress messages M3RL discarded because of an internal buffer overflow.</td>
<td>5 min</td>
</tr>
<tr>
<td>M3RLStackQueueFull</td>
<td>Number of messages that were discarded because the M3RL Stack Event Queue was full.</td>
<td>5 min</td>
</tr>
<tr>
<td>M3RLNetMgtQueueFull</td>
<td>Number of M3RL network management messages (SI=0)</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>TxM3RLDestUnknown</td>
<td>The number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxM3RLDestUnavail</td>
<td>The number of egress messages M3RL discarded because the RSP/Destination was Unavailable.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxM3RLDestCong</td>
<td>The number of egress messages M3RL discarded because the RSP/Destination’s congestion level was higher than the message’s priority.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**TxM3RLDestUnknown**

**Measurement Group:** Server MTP3 Exception  
**Measurement Type:** Simple  
**Description:** The number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.  
**Collection Interval:** 5 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
If a high number of these errors occurs, then an internal routing table problem exists. Contact My Oracle Support (MOS) for assistance.

**TxM3RLDestUnavail**

**Measurement Group:** Server MTP3 Exception  
**Measurement Type:** Simple  
**Description:** The number of egress messages M3RL discarded because the RSP/Destination was Unavailable.  
**Collection Interval:** 5 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
The RSP/Destination can be unavailable when the request is received from the User Part or while M3RL is buffering messages for a rerouting or changeover/changeback procedure.

**TxM3RLDestCong**

**Measurement Group:** Server MTP3 Exception  
**Measurement Type:** Simple  
**Description:** The number of egress messages M3RL discarded because the RSP/Destination’s congestion level was higher than the message’s priority.  
**Collection Interval:** 5 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
This value provides a measure of how many egress messages M3RL discarded because the RSP/Destination’s congestion level was higher than the message’s priority. Network Management
messages have the highest message priority. User Part message priorities are determined by the SCCP layer.

**TxM3RLBufOverflow**

**Measurement Group:** Server MTP3 Exception  
**Measurement Type:** Simple  
**Description:** The number of egress messages M3RL discarded because of an internal buffer overflow.  
**Collection Interval:** 5 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. This condition should not occur but may be caused by an unusually high setting of the T1, T3, or T6 timers. The default value is 60ms but the user has the ability to set them as high as 2000ms. You can view and modify the current M3RL timer values via the GUI under **SS7/Sigtran>Configuration>MTP3 Options.**  
2. An internal overflow condition may occur if the IP network is unstable causing M3RL to invoke multiple Changeover/Changeback procedures as links fail and recover. 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. Contact *My Oracle Support (MOS)* for assistance if needed.

**RxM3RLInvalidDPC**

**Measurement Group:** Server MTP3 Exception  
**Measurement Type:** Simple  
**Description:** This value provides a measure of how many ingress messages are discarded because the DPC was not a True Point Code (TPC) or Capability Point Code (CPC) configured for the MP.  
**Collection Interval:**  
**Recovery:**  
1. From the GUI main menu under **SS7/Sigtran>Configuration>Link Sets** verify that the LSP Point Code field is set to *All* if signaling can arrive for either CPC or TPC on this link set.  
2. If this measurement is large, it may indicate a routing inconsistency between STP/SG and the MP. You can view the point codes of the MP from **SS7/Sigtran>Configuration>Local Signaling Points.**

**RxM3RLInvalidSI**

**Measurement Group:** Server MTP3 Exception  
**Measurement Type:** Simple
**Description:** This value provides a measure of how many ingress messages M3RL discarded because the Service Indicator received was not 0 (SNM) or 3 (SCCP).

**Collection Interval:** 5 min

**Measurement Scope:** NE, Server

**Recovery:**

This type of failure should never occur and usually indicates that the routing in the STP/SG or originator of the message is incorrect.

### RxM3RLInvalidNI

**Measurement Group:** Server MTP3 Exception

**Measurement Type:** Simple

**Description:** This value provides a measure of how many ingress messages M3RL discarded because the Network Indicator received was the same value configured for the MP.

**Collection Interval:** 5 min

**Measurement Scope:** NE, Server

**Recovery:**

If this measurement is large, it may indicate a routing inconsistency between the STP/SG and the MP. The NI values for the MP can be viewed via the GUI main menu under SS7/Sigtran>Configuration>Local Signaling Points. See the SS7 Domain column.

### RxM3RLBufOverflow

**Measurement Group:** Server MTP3 Exception

**Measurement Type:** Simple

**Description:** This value provides a measure of how many ingress messages M3RL discarded because of an internal buffer overflow.

**Collection Interval:** 5 min

**Measurement Scope:** NE, Server

**Recovery:**

This should never occur unless the MP is experiencing severe overload conditions and SCCP is unable to service its event queue.

### M3RLStackQueueFull

**Measurement Group:** Server MTP3 Exception

**Measurement Type:** Simple

**Description:** The number of messages that were discarded because the M3RL Stack Event Queue was full. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

**Collection Interval:** 5 min
Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

M3RLNetMgtQueueFull

Measurement Group: Server MTP3 Exception

Measurement Type: Simple

Description: The number of M3RL network management messages (SI=0) that were discarded because the M3RL Network Management Event Queue was full. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

Server MTP3 Performance measurements

Table 99: Server MTP3 Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxM3RLDataMsgs</td>
<td>Egress M3RL DATA Messages (at M3RL-&gt;M3UA interface). This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxM3RLDataMsgs</td>
<td>Ingress M3RL DATA Messages (at M3RL-&gt;M3UA interface). This measurement includes SCMG messages (which are DATA to the M3RL layer), but</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>M3RLStackQueuePeak</td>
<td>Peak M3RL Stack Event Queue utilization (0-100%) measured during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>M3RLStackQueueAvg</td>
<td>Average M3RL Stack Event Queue utilization (0-100%) measured during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>M3RLNetMgtQueuePeak</td>
<td>Peak M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval</td>
<td>5 min</td>
</tr>
<tr>
<td>M3RLNetMgtQueueAvg</td>
<td>Average M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval</td>
<td>5 min</td>
</tr>
</tbody>
</table>

**TxM3RLDataMsgs**

**Measurement Group:** Server MTP3 Performance

**Measurement Type:** Simple

**Description:** This value provides a measure of how many egress DATA messages are sent from M3RL to M3UA. This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.

**Collection Interval:** 5 min

**Peg Condition:** This counter is pegged each time a M3RL DATA message is sent to M3UA. This counter includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

**RxM3RLDataMsgs**

**Measurement Group:** Server MTP3 Performance

**Measurement Type:** Simple

**Description:** This value provides a measure of how many ingress DATA messages M3RL is processing from the network. This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SSNM messages.

**Collection Interval:** 5 min
**M3RLStackQueuePeak**

**Measurement Group:** Server MTP3 Performance  
**Measurement Type:** Max  
**Description:** The peak M3RL Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum M3RL Stack Event Queue utilization sample taken during the collection interval.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.  
3. Contact [My Oracle Support (MOS)](mailto:Support) for assistance if needed.

**M3UAStructQueueAvg**

**Measurement Group:** Server M3UA Performance  
**Measurement Type:** Average  
**Description:** The average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.  
**Collection Interval:** 30 min  
**Peg Condition:** The average of all M3UA Stack Event Queue utilization samples taken during the collection interval.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

3. Contact My Oracle Support (MOS) for assistance if needed.

M3RLNetMgtQueuePeak

Measurement Group: Server MTP3 Performance

Measurement Type: Max

Description: The peak M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Peg Condition: The maximum M3RL Network Management Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

M3RLNetMgtQueueAvg

Measurement Group: Server MTP3 Performance

Measurement Type: Average

Description: The average M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 5 min

Peg Condition: The average of all M3RL Network Management Event Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.
Server Resource Usage measurements

Table 100: Server Resource Usage Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS7ProcessPeak</td>
<td>Peak SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.</td>
<td>5 min</td>
</tr>
<tr>
<td>SS7ProcessAvg</td>
<td>Average SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.</td>
<td>5 min</td>
</tr>
<tr>
<td>SS7RxMsgRatePeak</td>
<td>Peak Ingress Message Rate (in messages per second) measured during the collection interval. The Ingress Message Rate is the number of non-SNM (SI &gt; 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.</td>
<td>5 min</td>
</tr>
<tr>
<td>SS7RxMsgRateAvg</td>
<td>Average Ingress Message Rate (messages per second) during the collection interval. The Ingress Message Rate is the number of non-SNM (SI &gt; 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.</td>
<td>5 min</td>
</tr>
<tr>
<td>ITUPDUUUtilPeak</td>
<td>The peak ITUI/ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>ITUPDUUUtilAvg</td>
<td>The average ITUI/ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>ANSIPDUUUtilPeak</td>
<td>The peak ANSI PDU Buffer Pool utilization (0-100%) measured during the collection interval.</td>
<td>5 min</td>
</tr>
<tr>
<td>ANSIPDUUUtilAvg</td>
<td>The average ANSI PDU Buffer Pool utilization (0-100%)</td>
<td>5 min</td>
</tr>
</tbody>
</table>
### SS7ProcessPeak

**Measurement Group:** Server Resource Usage  
**Measurement Type:** Max  
**Description:** The peak SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 Process is responsible for all SS7-related processing.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum SS7 Process CPU utilization sample taken during the collection interval.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.  
3. Contact My Oracle Support (MOS) for assistance if needed.

### SS7ProcessAvg

**Measurement Group:** Server Resource Usage  
**Measurement Type:** Average  
**Description:** The average SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all SS7 Process CPU utilization samples taken during the collection interval.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.  
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.  
3. Contact My Oracle Support (MOS) for assistance if needed.
**SS7RxMsgRatePeak**

**Measurement Group:** Server Resource Usage

**Measurement Type:** Max

**Description:** The peak Ingress Message Rate (in messages per second) measured during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.

**Collection Interval:** 5 min

**Peg Condition:** The maximum Ingress Message Rate (messages per second) sample taken during the collection interval

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
2. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing mis-configuration problem may exist.
4. Contact *My Oracle Support (MOS)* for assistance if needed.

**SS7RxMsgRateAvg**

**Measurement Group:** Server Resource Usage

**Measurement Type:** Max

**Description:** The average Ingress Message Rate (messages per second) during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.

**Collection Interval:** 5 min

**Peg Condition:** The average of all Ingress Message Rate samples taken during the collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

1. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
2. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing mis-configuration problem may exist.
4. Contact *My Oracle Support (MOS)* for assistance if needed.
**ItuiPDUUtilPeak**

**Measurement Type:** Max  
**Measurement Group:** Server Resource Usage  
**Description:** The peak ITUI/ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The maximum SS7 ITUI/ITUN PDU Buffer Pool utilization sample taken during the collection interval.  
**Measurement Scope:** NE, Server  

**Recovery:**  
1. ITUI PDU is allocated to each ITUI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.  
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.  
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).  
4. Contact *My Oracle Support (MOS)* for assistance if needed.

**ITUPDUUtilAvg**

**Measurement Type:** Average  
**Measurement Group:** Server Resource Usage  
**Description:** The average ITUI/ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.  
**Collection Interval:** 5 min  
**Peg Condition:** The average of all SS7 ITUI/ITUN PDU Buffer Pool utilization samples taken during the collection interval.  
**Measurement Scope:** NE, Server  

**Recovery:**  
1. ITUI PDU is allocated to each ITUI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.
2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

4. Contact My Oracle Support (MOS) for assistance if needed.

ANSIPDUUtilPeak

**Measurement Group:** Server Resource Usage

**Measurement Type:** Max

The peak ANSI PDU Buffer Pool utilization (0-100%) measured during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** The maximum ANSI PDU buffer pool utilization sample taken during the collection interval.

**Measurement Scope:** NE, Server

**Recovery:**

1. ANSI PDU is allocated to each ANSI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.

2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

4. Contact My Oracle Support (MOS) for assistance if needed.

AnsiPDUUtilAvg

**Measurement Group:** Server Resource Usage

**Measurement Type:** Average

**Description:** The average ANSI PDU Buffer Pool utilization (0-100%) measured during the collection interval.

**Collection Interval:** 5 min

**Peg Condition:** The average of all ANSI PDU buffer pool utilization samples taken during the collection interval.
Measurement Scope: NE, Server

Recovery:

1. ANSI PDU is allocated to each ANSI message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general PDU buffers are engineered for required SS7 domains and the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal SS7 queues.

2. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or SS7 Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or SS7) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.

3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).

4. Contact My Oracle Support (MOS) for assistance if needed.

Server SCCP Exception measurements

Table 101: Server SCCP Exception Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvError</td>
<td>Number of error log events.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvVital</td>
<td>Number of vital log events.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPInvalidDPC</td>
<td>Number of ingress messages SCCP discarded because the DPC is not the TPC or CPC of an MP for an ingress SCCP message.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPInvalidSSN</td>
<td>Number of ingress messages SCCP discarded because the CdPA SSN or affected SSN is missing/invalid for an ingress SCCP message.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPInvalidMsg</td>
<td>Number of ingress messages SCCP discarded because the Message Type is not currently supported.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

Note: Only the following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. Valid SCMG Message Types: SSA, SSP, SST.
<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxSCCPInvalidHop</td>
<td>Number of ingress messages SCCP discarded because of a Hop Counter violation associated with CdPA RI=route on GT.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPPInvalidClass</td>
<td>Number of ingress messages SCCP discarded because of an invalid protocol class. Note: Only classes 0 and 1 are supported.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
| RxSCCPInvalidGTI    | Number of ingress messages SCCP discarded because an invalid Global Title Indicator (GTI) value was received. This only applies to messages received with RI=route on GT.  
   **Note:** GTI=0 is invalid. (Applications using AWPSS7 may impose further limitations on GTI values. For example, EXHR supports: only GTI=2 for ANSI, only GTI=2 and GTI=4 for ITU). | 30 min              |
| RxMPCongestion      | Number of ingress SCCP messages that were discarded because of Local MP Congestion. | 30 min              |
| RxMaxTpsExceeded    | Number of ingress SCCP messages that were discarded because of the Local MP Maximum TPS limit. | 30 min              |
| TxSCCPCongestion    | Number of egress messages SCCP discarded because the RSP/Destination's congestion level was higher than the message's priority. | 30 min              |
| TxSCCPInvalidDPC    | Number of egress messages SCCP discarded because the RSP/DPC is missing or invalid for an egress SCCP message. | 30 min              |
| TxSCCPInvalidSSN    | Number of egress messages SCCP discarded because the remote SSN is missing or invalid for an egress SCCP message. | 30 min              |
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCPStackQueueFull</td>
<td>Number of ingress SCCP messages that were discarded because the SCCP Stack Event Queue was full.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCCPUnavailDPC</td>
<td>RSP/affected DPC unavailable for an egress SCCP message.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCCPUnknownDPC</td>
<td>RSP/affected DPC unknown (unequipped) for an egress SCCP message.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCCPUnavailSSN</td>
<td>Remote/affected SSN unavailable for an egress SCCP message.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCCPUnknownSSN</td>
<td>Remote/affected SSN unknown (unequipped) for an egress SCCP message.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCCPInvUserMsgs</td>
<td>Invalid N-UnitDatareq received from the Local SCCP User/application.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPUnavailSSN</td>
<td>Messages received for a prohibited Local/Affected SSN.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPUnknownSSN</td>
<td>Messages received for an unequipped/unknown Local/Affected SSN.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCMGErrors</td>
<td>Number of ingress/egress malformed or unsupported messages.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCCPGTTFailure</td>
<td>Default action for ri=rt-on-gtt messages from the SS7 stack.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**EvError**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of error trace conditions. This indicates that an expected but abnormal path was taken in the software, which warrants further investigation.

By default, error tracing is disabled. Non-zero values in this measurement indicate that something is occurring that would have generated an error trace, were error tracing enabled. These error trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

**Collection Interval:** 30 min
**EvVital**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of vital trace conditions encountered. A vital trace indicates that an unexpected path was taken in the software, which warrants further investigation. These vital trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

During application start-up and shutdown, vital traces are used to show details that can aid in debugging of initialization and shutdown problems. These traces are always enabled and cannot be turned off.

It is a VITAL error condition for any other instance.

**Collection Interval:** 30 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
Contact *My Oracle Support (MOS)* for assistance if any unexpected non-zero values in this measurement occur.

**RxMaxTpsExceeded**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress SCCP messages that were discarded because of the Local MP Maximum TPS limit.

**Collection Interval:** 30 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. The MP is approaching or exceeding its engineered traffic handling capacity. 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 Status**.

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 the GUI main menu under **Status & Manage>KPI Display**. 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 the GUI main menu under **Status & **
Manage>KPI Display. 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. Examine the alarm log from the GUI main menu under Alarms & Events.

5. Contact My Oracle Support (MOS) for assistance if needed.

RxMPCongestion
Measurement Group: Server SCCP Exception
Measurement Type: Simple
Description: The number of ingress SCCP messages that were discarded because of local MP congestion.
Collection Interval: 30 min
Measurement Scope: NE, Server
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 & Control>Server Status.
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 the GUI main menu under Status & Control>KPI Display. 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 the GUI main menu under Status & Control>KPI Display. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The SS7 process may be experiencing problems. The alarm log should be examined from the GUI main menu under Alarms & Events.
5. Contact My Oracle Support (MOS) for assistance if needed.

RxSCCPInvalidDPC
Measurement Group: Server SCCP Exception
Measurement Type: Simple
Description: The number of ingress messages SCCP discarded because the MTP point code was present but was not a TPC or CPC for the signaling standard of the message.
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:
This count shows how many ingress messages SCCP discarded because the point code received in the MTP was not encoded correctly (same as TPC or CPC) for the signaling standard of the message. If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured. Contact My Oracle Support (MOS) for assistance.
RxSCCPInvalidSSN

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress messages SCCP discarded because the CdPA/CgPA SSN was present but had an invalid value (SSN< 1 or SSN >254).  
**Collection Interval:** 30 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured.

RxSCCPInvalidMsg

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress messages SCCP discarded because the message type is not currently supported.  
**Note:** Only the following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. Valid SCMG message types are SSA, SSP, and SST.  
**Collection Interval:** 30 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
If a high number of these errors occurs, then the originator of the message may be misconfigured.

RxSCCPInvalidHop

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** Number of ingress messages SCCP discarded because of a Hop Counter violation associated with CdPA RI=route on GT.  
**Collection Interval:** 30 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
If this error occurs, then either the originator of the message is setting the initial value too low or the STPs are rerouting the message too many times due to a possible STP routing misconfiguration. Contact *My Oracle Support (MOS)* for assistance.
**RxSCCPInvalidClass**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress messages SCCP discarded because of an invalid protocol class.  
**Note:** Only classes 0 and 1 are supported.  
**Collection Interval:** 30 min  
**Measurement Scope:** NE, Server  
**Recovery:**  
If a high number of these errors occurs, then the originator of the message may be misconfigured or the network is misconfigured causing mis-routing of messages.

**RxSCCPInvalidGTI**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of ingress messages SCCP discarded because an invalid Global Title Indicator (GTI) value was received. This only applies to messages received with RI=route on GT.  
**Note:** GTI=0 is invalid.  
**Collection Interval:** 30 min  
**Peg Condition:**  
**Measurement Scope:** NE, Server  
**Recovery:**  
If a high number of these errors occurs, then the originator of the message may be misconfigured.

**RxSCCPReassFAIL**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of times the reassembly procedure failed.  
**Collection Interval:** 30 min  
**Peg Condition:** For each reassembly failure for ingress segmented XUDT message received from network  
**Measurement Scope:** Network, NE, Server  
**Recovery:**  
1. This value provides a measure of number of reassembly procedure failures encountered during the reporting interval.  
2. Check for any related additional Events or Alarms from the server.
**RxSCCPReassInternalFail**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of reassembly procedure failures due to internal error or resource limitation.  
**Collection Interval:** 30 min  
**Peg Condition:** N/A  
**Measurement Scope:** Network, NE, Server  
**Recovery:**  
1. This value provides a measure of number of reassembly procedure failures encountered due to errors encountered on server, during the reporting interval.  
2. Non-zero value for this measurement tag represents resource usage issues on the server. Check for any related additional Events or Alarms from the server.

**RxSCCPReassOOSFail**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of reassembly procedure failures due to out-of-sequence segments received from network.  
**Collection Interval:** 30 min  
**Peg Condition:** For each ongoing reassembly procedure failure as a result of out of order arrival of remaining segments.  
**Measurement Scope:** Network, NE, Server  
**Recovery:**  
1. This value provides a measure of number of reassembly procedure failures encountered due to “out of order arrival of remaining segments in a reassembly procedure” reason, during the reporting interval.  
2. Non-zero value for this measurement tag represents sequencing issues in packet arrival from network or any other routing error or delays in network or on server. Check for any related additional Events or Alarms from the server.

**RxSCCPReassTExp**

**Measurement Group:** Server SCCP Exception  
**Measurement Type:** Simple  
**Description:** The number of reassembly procedure failures due to reassembly timer expiry.  
**Collection Interval:** 30 min  
**Peg Condition:** For each reassembly procedure failures due to reassembly timer expiry  
**Measurement Scope:** Network, NE, Server
Recovery:

1. This value provides a measure of number of reassembly procedure failures encountered due to “Reassembly Timer Expiry” reason, during the reporting interval.

2. Non-zero value for this measurement tag represents latency issues in packet arrival from network or any other delay on server resulting in reassembly timer expiry. Check for any related additional Events or Alarms from the server.

RxSCCPSegmentOOS

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of XUDT segments received out-of-sequence from network.

Collection Interval: 30 min

Peg Condition: On received XUDT segments with F bit set as 0 and received segments could not be attached to any open reassembly procedure (i.e. reassembly procedure was not started for this and no key found to associate the segments to an in-process reassembly)

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of number of segmented XUDT messages received with sequence delivery option but arrived out of sequence at SCCP Layer, during the reporting interval.

2. For these out of sequence received XUDT segments, there is no ongoing reassembly procedure to attach these segments.

3. Non-zero value for this measurement tag represents in-sequence routing or reassembly key uniqueness issue. Check for any related additional Events or Alarms from the server.

RxSCCPUnavailSSN

Measurement Group: Server SCCP Exception

Measurement Type: Simple

Description: The number of partially reassembled segments discarded due to any errors.

Collection Interval: 30 min

Peg Condition: For each segmented XUDT message that was buffered and discarded due to reassembly procedure failure

Measurement Scope: Network, NE, Server

Recovery:

This value provides cumulative measure of ingress segmented XUDT messages which were buffered but discarded due to reassembly procedure failure.
Measurement Type: Simple
Description: Number of ingress messages (RI=SSN) SCCP discarded because the CdPA SSN (Local SSN for MPs TPC) was manually disabled.
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:
This value provides a measure of how many ingress (RI=SSN) messages SCCP discarded because the affected Local Subsystem status was manually disabled. The Status of Local Subsystems (Local SCCP Users, LSUs) for a Local Signaling Point can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Local SCCP Users'.

RxSCCPUnknownSSN
Measurement Group: Server SCCP Exception
Measurement Type: Simple
Description: Number of ingress messages (RI=SSN) SCCP discarded because the CdPA SSN (Local SSN for MPs TPC) is not configured for the MTP DPC's signaling domain
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:
This value provides a measure of how many ingress (RI=SSN) messages SCCP discarded because the affected Local Subsystem is not configured for the MTP DPC's signaling domain. The Local Subsystems (Local SCCP User, LSUs) for a Local Signaling Point can be configured via the following GUI menu: Main Menu: SS7/SIGTRAN -> Configuration -> 'Local SCCP Users' Insert.

RxSCCPXudtInvSgmnt
Measurement Group: Server SCCP Exception
Measurement Type: Simple
Description: The number of received XUDT segments resulted in protocol violation decode error.
Collection Interval: 30 min
Peg Condition: For protocol decoding errors while parsing ingress segmented XUDT
Measurement Scope: Network, NE, Server
Recovery:
This value provides a measure of malformed segmented XUDT messages received from the network.

SCCPGTTFailure
Measurement Group: Server SCCP Exception
Measurement Type: Simple
**SCCPGTTFailures**

**Description:** Count of SCCP GTT Failures due to default GTT handling in SS7Stack.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:** This value provides a measure of how many "ri=rt-ongt" messages were subject to default Global Title Translation processing. This can occur when Application is using SS7 Stack for processing only "rt-on-ssn" messages OR "rt-on-gt" message handling is not implemented in Application.

---

**SCCPStackQueueFull**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** The number of ingress SCCP messages that were discarded because the SCCP Stack Event Queue was full.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP are significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist.

3. Contact My Oracle Support (MOS) for assistance if needed.

---

**SCMGErrors**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** Number of ingress/egress malformed or unsupported messages.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

This value provides a measure of how many malformed or unsupported SCCP management messages were discarded. Supported SCMG messages are SST, SSP and SSA. Any other SCCP Management message is pegged under this tag.

---

**TxSCCPCongestion**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple
Measurements

**Description:** The number of egress messages SCCP discarded because the RSP/Destination's congestion level was higher than the message's priority.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**
You can view the remote RSPPs/Destinations to SCCP and their congestion status from the GUI main menu under SS7/Sigtran>Maintenance>Remote MTP3 Users.

**TxSCCPInvUserMsgs**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** SCCP User submitted an Invalid/malformed/unsupported message for egress routing (SCCP User->SCCP N-UnitDataReq)

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**
This value provides a measure of how many egress SCCP User messages encountered validation failure on SCCP. If a high number of these errors occur, then it indicates an encoding error at the originator or the originator of the message may be mis-configured.

**TxSCCPIvalidDPC**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** The number of egress messages SCCP discarded because the CdPA signaling point code is present but is not valid for the signaling standard of the message.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**
If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured.

**TxSCCPIvalidSSN**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** The number of egress messages SCCP discarded because the CdPA/CgPA SSN was present but had an invalid value (SSN< 1 or SSN >254).

**Collection Interval:** 30 min
Measurements

**Measurement Scope:** NE, Server

**Recovery:**

If a high number of these errors occurs, it indicates that an encoding error exists at the originator or that the originator of the message may be misconfigured.

**TxSCCPSegmentFAIL**

**Measurement Group:** Server SCCP Performance

**Measurement Type:** Simple

**Description:** The number of times segmentation procedure failed.

**Collection Interval:** 30 min

**Peg Condition:** On failure in completion of segmentation procedure for each large egress user data message.

**Measurement Scope:** Network, NE, Server

**Recovery:**

1. This value provides a measure of number of segmentation procedure completion failures for large egress user data messages. Segmentation Error Procedure is executed on each such failure.
2. Check for any related additional Events or Alarms from the server.

**TxSCCPUnavailDPC**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** Number of egress messages SCCP discarded because the affected DPC status was marked prohibited/unavailable.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

This value provides a measure of how many egress messages SCCP discarded because the RSP/Destination status was paused / prohibited at SCCP. Point code status is received from M3RL via the MTP-PAUSE and MTP-RESUME indications. The remote RSPs/Destinations known to SCCP and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote Signaling Points'.

**TxSCCPUnavailSSN**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** Number of egress messages SCCP discarded because the CdPA or Affected SSN was either marked prohibited/unavailable.

**Collection Interval:** 30 min
Measurements

**Measurement Scope:** NE, Server

**Recovery:**

This value provides a measure of how many egress messages SCCP discarded because the Remote Subsystem status was Prohibited. Subsystem status is received from M3RL via the SS-STATUS indications or via SCMG SSA and SSP messages. The remote subsystems (RMUs) known to SCCP and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote MTP3 Users'.

**TxSCCPUnknownDPC**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** Number of egress messages SCCP discarded because the affected DPC in message is not configured or is unknown.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

This value provides a measure of how many egress messages SCCP discarded because the RSP or affected DPC in the message is not configured and is unknown at SCCP. The remote RSPs/affected Destinations known to SCCP and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote Signaling Points'.

**TxSCCPUnknownSSN**

**Measurement Group:** Server SCCP Exception

**Measurement Type:** Simple

**Description:** Number of egress messages SCCP discarded because the CdPA or affected SSN was unknown.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

This value provides a measure of how many egress messages SCCP discarded because the Subsystem was unknown to SCCP. The remote subsystems (RMUs) can be configured from GUI menu: Main Menu: SS7/SIGTRAN -> Configuration->Remote MTP3 Users and their status can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Remote MTP3 Users'.


# Server SCCP Performance measurements

Table 102: Server SCCP Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxSCCPMsgs</td>
<td>Egress messages sent by SCCP to M3RL (SCCP&gt;M3RLMTP-TRANSFER request).</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPMsgs</td>
<td>Ingress messages received by SCCP from M3RL (M3RL&gt;SCCP MTP-TRANSFER indication).</td>
<td>30 min</td>
</tr>
<tr>
<td>SCCPStackQueuePeak</td>
<td>Peak SCCP Stack Event Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SCCPStackQueueAvg</td>
<td>Average SCCP Stack Event Queue utilization (0-100%) measured during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCCPUserMsgs</td>
<td>Valid N-UnitDatareq generated by local SCCP User and processed by SCCP.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxSCMGMgs</td>
<td>Number of valid egress SCMG messages.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPUserMsgs</td>
<td>UDT/XUDT received and N-UnitDataInd Event delivered to Local SCCP.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCCPUserNoticeMsgs</td>
<td>User UDTS/XUDTS received and NNotice-Ind sent to Local SCCP User.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxSCMGMgs</td>
<td>Number of valid ingress SCMG messages.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxMsgRateAvg</td>
<td>The average Egress Message Rate (messages per second) during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>TxMsgRatePeak</td>
<td>The peak Egress Message Rate (in messages per second) measured during the collection interval.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TxSCCPLargeMsgs**

*Measurement Group:* Server SCCP Performance
Measurements

**Measurement Type:** Simple

**Description:** The number of egress large user data messages for segmentation.

**Collection Interval:** 30 min

**Peg Condition:** For each large user data message submitted by SCCP User for egress routing.

**Measurement Scope:** Network, NE, Server

**Recovery:**

This value provides a measure of how many large user data messages are submitted to SCCP layer for egress routing during the reporting interval. This measurement peg value divided by the interval yields the average rate of large egress user data messages for the server.

**TxSCCPMsgs**

**Measurement Group:** Server SCCP Performance

**Measurement Type:** Simple

**Description:** Egress messages sent by SCCP to M3RL (SCCP->M3RL MTP-TRANSFER request). This value provides a measure of how many egress SCCP messages are being processed by the MP server.

**Collection Interval:** 30 min

**Measurement Scope:** NE, Server

**Recovery:**

No action required.

**TxSCCPSegmentsPerMsg**

**Measurement Group:** Server SCCP Performance

**Measurement Type:** Simple

**Description:** The number of segments created for each large egress user data message.

**Collection Interval:** 30 min

**Peg Condition:** When the segmentation procedure is completed on each large egress user data packet, using “number of segments” as index.

**Measurement Scope:** Network, NE, Server

**Recovery:**

1. Values in this arrayed measurement provides a measure of number of XUDT messages created each time a large user data messages is segmented by SCCP layer.
2. This arrayed measurement can be used for heuristics on segments created during the reporting interval and the SS7 traffic rate impact due to large egress user data size traffic.

**TxSCCPSegmentSUCC**

**Measurement Group:** Server SCCP Performance

**Measurement Type:** Simple
Description: The number of times segmentation procedure completed successfully.
Collection Interval: 30 min
Peg Condition: On successful completion of segmentation procedure for each large egress user data message (i.e. user data length is greater than SCCP Option Configured value).
Measurement Scope: Network, NE, Server
Recovery:

This value provides a measure of number of successful segmentation procedure completion for large egress user data messages are successfully segmented and corresponding XUDT messages are forwarded by SCCP layer for egress routing during the reporting interval.

TxSCCPUserMsgs
Measurement Group: Server SCCP Performance
Measurement Type: Simple
Description: Egress messages sent by SCCP User to SCCP to M3RL (SCCPUser-> SCCP N-UnitDataReq->M3RL MTP-TRANSFER request)
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:

This value provides a measure of how many egress SCCP User messages are being processed by the MP server.

TxSCMGMsgs
Measurement Group: Server SCCP Performance
Measurement Type: Simple
Description: The number of valid egress SCMG messages.
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:

This value provides a measure of egress SCCP Management messages This could be due to local or remote SCCP/SCCP Users status. The Status of Local or Remote Subsystems can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Local SCCP Users' or "Remote MTP3 Users".

RxSCCPMsgs
Measurement Group: Server SCCP Performance
Measurement Type: Simple
Description: Ingress messages received by SCCP from M3RL (M3RL> SCCP MTP TRANSFER indication).
Collection Interval: 30 min
Measurement Scope: NE, Server
Recovery:
No action required.

RxSCCPReassSUCC
Measurement Group: Server SCCP Performance
Measurement Type: Simple
Description: The number of times reassembly procedure successfully completed.
Collection Interval: 30 min
Peg Condition: On successful completion of reassembly procedure using a number of ingress segmented XUDT messages.
Measurement Scope: Network, NE, Server
Recovery:
This value provides a measure of number of successful reassembly procedure (using a number of ingress segmented XUDT messages) completion during the reporting interval. The reassembled user data is forwarded as single packet to SCCP User.

RxSCCPrtGtFrwdAppl
Measurement Group: Server SCCP Performance
Measurement Type: Simple
Description: The number of Rt On Gt Messages forwarded to Local Application.
Collection Interval: 30 min
Peg Condition: N/A
Measurement Scope: Network, NE, Server
Recovery:
This value provides a measure of number of messages received with CDPA RI=GT and are forwarded to Local Application due to configured SCCP Option.

RxSCCPrtGtXudtSgmnt
Measurement Group: Server SCCP Performance
Measurement Type: Simple
Description: The number of Rt on Gt segmented XUDT messages received from network
Collection Interval: 30 min
Peg Condition: N/A
Measurement Scope: Network, NE, Server
Recovery:

This value provides a measure of number of Rt on Gt segmented XUDT messages received from the network.

**RxSCCPRtSsnXudtSgmnt**

**Measurement Group:** Server SCCP Performance  
**Measurement Type:** Simple  
**Description:** The number of Rt on Ssn segmented XUDT messages received from network.  
**Collection Interval:** 30 min  
**Peg Condition:** N/A  
**Measurement Scope:** Network, NE, Server  
Recovery:  
This value provides a measure of number of Route on SSN segmented XUDT messages received from the network.

**RxSCCPSegmentSrvcMsg**

**Measurement Group:** Server SCCP Performance  
**Measurement Type:** Simple  
**Description:** The number of Segmented XUDTS messages received from network.  
**Collection Interval:** 30 min  
**Peg Condition:** For each segmented XUDTS messages received from network  
**Measurement Scope:** Network, NE, Server  
Recovery:  
This value provides a measure of number of segmented XUDTS messages received from the network.

**RxSCCPGmntReassPerMsg**

**Measurement Group:** Server SCCP Performance  
**Measurement Type:** Simple  
**Description:** The number of segments reassembled to create one large ingress user data message.  
**Collection Interval:** 30 min  
**Peg Condition:** This is an arrayed measurement with “number of XUDT segments assembled” as index. Peg this measurement using “number of XUDT segments assembled” as index, when reassembly procedure is completed using more than one ingress segmented XUDT message.  
**Measurement Scope:** Network, NE, Server  
Recovery:
1. Values in this arrayed measurement provides a measure of number of segmented XUDT messages were reassembled for each reassembly procedure before forwarding a large user data messages to SCCP User.

2. This arrayed measurement can be used for heuristics on number of segments network used for segmenting large message during the reporting interval and the SS7 traffic rate impact due to segmented XUDT messages on overall SCCP processing rate.

RxSCCPgmntsReassSUCC

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of XUDT segments reassembled successfully.

Collection Interval: 30 min

Peg Condition: For each well-formed ingress segmented XUDT message resulting in a successful reassembly procedure

Measurement Scope: Network, NE, Server

Recovery: This value provides a measure of well-formed ingress segmented XUDT messages that are reassembled successfully.

RxSCCPgmntXudtMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of ingress segmented XUDT messages received from network.

Collection Interval: 30 min

Peg Condition: For each segmented XUDT message received from network.

Measurement Scope: Network, NE, Server

Recovery:

1. This value provides a measure of how many segmented XUDT messages are received by SCCP layer during the reporting interval. SCCP will execute reassembly procedure for each such received message.

2. This measurement peg value divided by the interval yields the average rate of new segmented XUDT messages received from the network.

RxSCCPUserMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Ingress SCCP UDT/XUDT messages sent by SCCP to Configured and available SCCP Users using a local SSN (SCCP->SCCP User N-UnitDataInd)
Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many ingress SCCP User (RI=SSN) messages are being forwarded to SCCP User application hosted by the MP server.

RxSCCPUserNoticeMsgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: Ingress SCCP UDTS/XUDTS (RI=SSN) messages converted into N-Notice-Ind by SCCP and sent to the configured and available SCCP Users using a local SSN (SCCP->SCCP User N-NoticeInd)

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

1. This value provides a measure of how many ingress SCCP UDTS/XUDTS (RI=SSN) messages were received and converted into N-Notice-Ind and forwarded to SCCP User application hosted by the MP server.

2. If a high number of these errors occur, then it indicates the remote SCCP/SCCP Application could not process the message as expected and resulted in executing sccp error handling procedure. It’s normally associated with an event/alarm condition. If a high number of these errors occur, then check the event history under "Main Menu:: Alarms & Events-> View History".

RxSCMGMgs

Measurement Group: Server SCCP Performance

Measurement Type: Simple

Description: The number of valid ingress SCMG messages.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

This value provides a measure of ingress SCCP Management messages. This could be due to local or remote SCCP/SCCP Users status. The Status of Local or Remote Subsystems can be viewed via the following GUI menu: Main Menu: SS7/SIGTRAN -> Maintenance -> 'Local SCCP Users' or "Remote MTP3 Users".

SCCPStackQueuePeak

Measurement Group: Server SCCP Performance

Measurement Type: Max
Description: The peak SCCP Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The maximum SCCP Stack Event Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP are significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

SCCPStackQueueAvg

Measurement Group: Server SCCP Performance

Measurement Type: Average

Description: The average SCCP Stack Event Queue utilization (0-100%) measured during the collection interval. This measurement is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

Collection Interval: 30 min

Peg Condition: The average of all SCCP Stack Event Queue utilization samples taken during the collection interval.

Measurement Scope: NE, Server

Recovery:
1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact My Oracle Support (MOS) for assistance if needed.

TxMsgRateAvg

Measurement Group: Server Resource Usage

Measurement Type: Average

Description: The average Egress Message Rate (messages per second) during the collection interval.

Collection Interval: 30 min

Peg Condition: The average of all Ingress Message Rate samples taken during the collection interval.
**Measurement Scope**: NE, Server

**Recovery**:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.

3. Contact *My Oracle Support (MOS)* for assistance if needed.

**TxMsgRatePeak**

**Measurement Group**: Server Resource Usage

**Measurement Type**: Max

**Description**: The peak Ingress Message Rate (in messages per second) measured during the collection interval. The Ingress Message Rate is the number of non-SNM (SI > 0) messages that M3UA attempts to queue in the M3RL Stack Event Queue.

**Collection Interval**: 30 min

**Peg Condition**: The maximum Ingress Message Rate (messages per second) sample taken during the collection interval.

**Measurement Scope**: NE, Server

**Recovery**:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or an STP/SG routing misconfiguration problem may exist.

3. Contact *My Oracle Support (MOS)* for assistance if needed.

**SS7 Exception Measurements**

**Table 103: SS7 Exception Measurement Report Fields**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ss7TxFailedCA</td>
<td>Number of MAP response messages failed to transfer from SS7 TCAP layer to comagent layer.</td>
<td>30 min</td>
</tr>
<tr>
<td>Ss7TxMpUnkdiscard</td>
<td>Unknown SS7 MP id. Failed to transfer MAP response message. MP id from origination</td>
<td>30 min</td>
</tr>
</tbody>
</table>
**Ss7TxFailedCA**

**Measurement Group:** SS7 Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** The number of MAP response messages successfully transferred from SS7 TCAP layer to ComAgent layer  
**Collection Interval:** 30 min  
**Peg Condition:** When TCAP layer successfully forwards message to Communication Agent.  
**Measurement Scope:** Network, NE, Server  
**Recovery:** Values in this measurement provide a measure of number of TCAP messages send failed to Communication Agent. Non-zero value for this measurement tag represents resource usage issues on the server. Check for any related additional Events or Alarms from the server.

**Ss7TxMpUnkDiscard**

**Measurement Group:** SS7 Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Single  
**Description:** Unknown SS7 MP ID. Failed to transfer MAP response message. MP ID from origination transaction ID can not be mapped to any SS7 MP in topology  
**Collection Interval:** 30 min  
**Peg Condition:** When TCAP layer fails to find other XG SS7 MP information in database.  
**Measurement Scope:** Network, NE, Server  
**Recovery:** Values in this measurement provide a measure of number of TCAP messages discarded by TCAP layer when it is not able to find the XG SS7 MP information. Non-zero value for this measurement tag represents resource usage issues on the server. Check for any related additional Events or Alarms from the server.
SS7 Performance Measurements

Table 104: SS7 Performance Measurement Report Fields

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ss7TxSuccCA</td>
<td>Number of MAP response messages successfully transferred from SS7 TCAP layer to ComAgent layer</td>
<td>30 min</td>
</tr>
</tbody>
</table>

Ss7TxSuccCA

Measurement Group: SS7 Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of MAP response messages successfully transferred from SS7 TCAP layer to ComAgent layer.

Collection Interval: 30 min

Peg Condition: When TCAP layer successfully forwards message to Communication Agent.

Measurement Scope: Network, NE, Server

Recovery:

Values in this measurement provides a measure of number of TCAP messages forwarded to Communication Agent for routing to other XG SS7 Stack

Transport Manager Measurements

Table 105: Measurement Summary

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxTrFarEndClose</td>
<td>Number of times the far-end closed the association</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>EvTrManClose</td>
<td>Number of times the Trasnport was manually closed. This includes manual changes of the transport administrative state that cause the</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
<td>Group</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>transport to transition from APP-UP to Disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EvTrNoRespClose</td>
<td>Number of times the Transport was closed due to lack of response from the far-end. This includes lack of response to any signaling sent on the transport.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>EvTrCnxSuccess</td>
<td>The number of times the SCTP connection was successfully established on the Transport.</td>
<td>30 min</td>
<td>Transport Usage</td>
</tr>
<tr>
<td></td>
<td>The number of times the UDP socket in Listen Mode was opened successfully on the Transport.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EvTrCnxFail</td>
<td>The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td></td>
<td>The number of times open attempt on UDP socket in Listen Mode failed on the Transport.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TxTrSendFail</td>
<td>The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>RxTrRcvFailed</td>
<td>The number of times an SCTP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
</tbody>
</table>

E53474 Revision 01, July 2014
<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvTrSockInitFail</td>
<td>Number of times the socket initialization failed</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>TxTrOctets</td>
<td>The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>RxTrOctets</td>
<td>The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>TmTrEnaNotUp</td>
<td>The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.</td>
<td>30 min</td>
<td>Transport Usage</td>
</tr>
<tr>
<td>RxTmSctpBufAvg</td>
<td>The Average Value of the number of bytes in SCTP RX Window.</td>
<td>5 min</td>
<td>Transport Usage</td>
</tr>
<tr>
<td>RxTmSctpBufPeak</td>
<td>The Peak Value of the number of bytes in SCTP RX Window</td>
<td>5 min</td>
<td>Transport Usage</td>
</tr>
<tr>
<td>TmSingleTransQueuePeak</td>
<td>The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>TmSingleTransQueueAvg</td>
<td>The average single Transport Writer Queue utilization (0-100%) measured during the collection interval</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
<td>Group</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>TmSingleTransQueueFull</td>
<td>The number of egress messages that were discarded because the singleTransport Writer Queue was full.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>SctpTransPeerCWNDPeak</td>
<td>The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>SctpTransPeerCWNDAvg</td>
<td>The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>SctpTransPeerSRTTPeak</td>
<td>The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>SctpTransPeerSRTTAvg</td>
<td>The average value of smoothed round trip time for the SCTP Transport address during the collection interval.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>SctpTransUnAckedDataPeak</td>
<td>The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>SctpTransUnAckedDataAvg</td>
<td>The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>SctpTransRTOPeak</td>
<td>The peak value of retransmission timeout in use for the SCTP Transport address</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>SctpTransRTOAvg</td>
<td>The average value of retransmission timeout in use for the SCTP Transport address</td>
<td>30 min</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>EvSctpAdjIPToDwn</td>
<td>Number of time configured IP Address of an Adjacent Node goes from Available to Unavailable.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>EvSctpTransRej</td>
<td>Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.</td>
<td>30 min</td>
<td>Transport Exception</td>
</tr>
</tbody>
</table>

### Per Transport Measurements

**Table 106: RxTrFarEndClose**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>RxTrFarEndClose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>Number of times the far end closed the SCTP connection</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• the far-end of the association closes the association by sending either SHUTDOWN or ABORT</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If the closing of the association was expected, no further action is necessary - the association will be recovered as soon as the far-end is ready to connect again. If the closing of the association was not expected:</td>
</tr>
</tbody>
</table>
• Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
• Look in the event history at Main Menu > Alarms & Events > View History for event 19404 - Far-end closed the Transport to determine exactly when the far-end closed the association.
• Look for other events for the association or MP server in the event history.
• Verify that IP connectivity still exists between the MP server and the SG.
• Verify whether the far-end of the association is undergoing maintenance.
• Contact My Oracle Support (MOS) for assistance if needed.

Table 107: EvTrManClose

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvTrManClose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of times the Transport was manually closed. This includes manual changes of the transport administrative state that cause the transport to transition from APP-UP to Disabled.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• A manual change is made to the transport administrative state from Enabled to Blocked or from Enabled to Disabled, causing the transport to transition out of APP-UP protocol state.</td>
</tr>
<tr>
<td></td>
<td>Note: This has a special meaning for SS7/M3UA where it is linked with ASP-UP.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If the transport is known to be under maintenance, then no further action is necessary. If the transport was not known to be under maintenance:</td>
</tr>
<tr>
<td></td>
<td>• Transport status can be viewed at Main Menu &gt; Transport Manager &gt; Maintenance &gt; Transport.</td>
</tr>
</tbody>
</table>
• View the event history at Main Menu -> Alarms & Events -> View History, looking for event 19406 - Local Transport maintenance state change. Event 19406 shows the manual transport state transitions and contains a time-stamp of when the change occurred.
• The security logs at Main Menu > Log Files > Security Logs can be searched using the time-stamp from the event history log to determine which login performed the manual state change on the association.
• Contact My Oracle Support (MOS) for assistance if needed.

Table 108: EvTrNoRespClose

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvTrNoRespClose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of times the transport was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the transport.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• An established Transport is closed by the MP server due to lack of response at the SCTP level from the far-end of the association</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If all is well, this measurement should have a zero value. If non-zero, the association has been closed due to lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the SG. Troubleshooting:</td>
</tr>
<tr>
<td></td>
<td>• Transport status can be viewed at Main Menu &gt; Transport Manager &gt; Maintenance &gt; Transport.</td>
</tr>
<tr>
<td></td>
<td>• Look in the event history at Main Menu &gt; Alarms &amp; Events &gt; View History for event 19405 - Transport closed due to lack of response.</td>
</tr>
</tbody>
</table>
- Verify IP connectivity between the MP server and the SG.
- Determine if the far-end of the association is congested, possibly causing slow response times on the association.
- Check the IP network between the MP server and the SG for excessive retransmissions.
- Contact My Oracle Support (MOS) for assistance if needed.

### Table 109: EvTrCnxSuccess

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvTrCnxSuccess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Usage</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of times the SCTP connection was successfully established on the transport. The number of times the UDP socket in Listen Mode was opened successfully on the Transport.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
</tbody>
</table>
| Peg Condition                        | This measurement shall be incremented by one each time:
  - the SCTP association reaches the APP-UP protocol state (i.e. the connection is successfully ESTABLISHED)
  - UDP socket in Listen Mode was opened successfully. |
| Measurement Scope (Network, NE, Server) | NE, Server |
| Customer Action                  | If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise... Troubleshooting:
  - Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
  - Look in the event history at Main Menu > Alarms & Events > View History for events related to the association or the MP server to determine what may have caused the Transport to fail.
  - Contact My Oracle Support (MOS) for assistance if needed. |
### Table 110: EvTrCnxFail

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvTrCnxFail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections. The number of times open attempt on UDP socket in Listen Mode failed on the Transport.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
</tbody>
</table>
| Peg Condition | This measurement shall be incremented by one each time:  
  - An SCTP connect attempt fails  
  - An UDP open attempt in Listen mode fails  
  - An SCTP open attempt in Listen mode fails |
| Measurement Scope (Network, NE, Server) | NE, Server |
| Customer Action | If all is well, this measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Peer IP Address at least once and failed to establish the SCTP connection. Troubleshooting:  
  - Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.  
  - Check the event history log at Main Menu > Alarms & Events > View History, looking for event 19402 - Failed to connect Transport. Event 19402 provides more details as to the actual cause of the failure.  
  - Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at Main Menu > Transport Manager > Configuration > Adjacent Node.  
  - Verify that the remote port configured at Main Menu > Transport Manager > Configuration > Transport for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections. |
• Verify the IP network connectivity between the MP server and the Adjacent Node.
• If the SG must be configured to connect to the MP server's IP address and port, verify that the SG configuration matches the association configuration at **Main Menu > Transport Manager > Configuration > Transport**.
• Contact *My Oracle Support (MOS)* for assistance if needed.

### Table 111: TxTrSendFail

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>TxETrSendFail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• an attempt to send signaling DATA fails for any reason and the information being sent cannot be mapped to a specific transport</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If all is well, this measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this Transport has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association. Troubleshooting:</td>
</tr>
<tr>
<td></td>
<td>• Transport status can be viewed at <strong>Main Menu &gt; Transport Manager &gt; Maintenance &gt; Transport</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Look in the event history log at <strong>Main Menu &gt; Alarms &amp; Events &gt; View History</strong> for event <strong>19407 - Failed to send Transport DATA Message</strong>. Event 19407 gives more information about exactly what caused the failure to send.</td>
</tr>
</tbody>
</table>
Verify that the IP network between the MP server and the Adjacent Node is functioning as expected.

- Contact My Oracle Support (MOS) for assistance if needed.

<table>
<thead>
<tr>
<th>Table 112: RxTrRcvFailed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Tag</td>
</tr>
<tr>
<td>Measurement Group (64 chars)</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
</tr>
<tr>
<td>Collection Interval</td>
</tr>
<tr>
<td>Peg Condition</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
</tr>
<tr>
<td>Customer Action</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Table 113: EvTrSockInitFail

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvTrSockInitFail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of times the socket initialization failed.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• one or more socket options cannot be set according to the settings in the transport’s configuration set</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If all is well, this measurement should have a zero value. A non-zero value indicates some problem with association setup prior to attempting to connect the association. If this occurs, look in Main Menu &gt; Alarms &amp; Events &gt; View History for event 19401 - Failed to configure Transport. Event 19401 provides details about exactly what part of the configuration failed. Please contact My Oracle Support (MOS) for further assistance.</td>
</tr>
</tbody>
</table>

### Table 114: TxTrOctets

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>TxTrOctets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by the number of octets in the message each time:</td>
</tr>
<tr>
<td></td>
<td>• A DATA/non-DATA message is successfully sent on the transport.</td>
</tr>
</tbody>
</table>
Measurements

<table>
<thead>
<tr>
<th>Measurement Scope (Network, NE, Server)</th>
<th>NE, Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Action</td>
<td>None. This measurement indicates the level of signaling octets that have been sent over the association during the reporting interval.</td>
</tr>
</tbody>
</table>

**Table 115: RxTrOctets**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>RxTrOctets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by the number of octets in the message each time:</td>
</tr>
<tr>
<td></td>
<td>• A DATA/non-DATA message is successfully received on the transport</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>None. This measurement indicates the level of signaling octets that have been received over the association during the reporting interval.</td>
</tr>
</tbody>
</table>

**Table 116: TmTrEnaNotUp**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>TmTrEnaNotUp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Duration</td>
</tr>
<tr>
<td>Measurement Description (512 chars)</td>
<td>The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
</tbody>
</table>

E53474 Revision 01, July 2014 925
Peg Condition

Time shall be accumulated for this measurement during the collection interval when all of the following are true:

- the association is in the ENABLED administrative state
- the association is not in the ASP-UP protocol state for M3UA and APP-UP for other Plugins.

Measurement Scope (Network, NE, Server)

NE, Server

Customer Action

If all is well, the value of this measurement should be zero or very low value. A high value indicates that the association was set to the Enabled administrative state, but was not able to reach the desired protocol state (APP-UP) due to some problem. Troubleshooting:

- Association status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
- Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address at Main Menu > Transport Manager > Configuration > Adjacent Node.
- Verify that the remote port configured at Main Menu > Transport Manager > Configuration > Transport > Configure for the association correctly identifies the port that the SG is listening on for SCTP connections.
- Verify the IP network connectivity between the MP server and the SG.
- If the Adjacent Node must be configured to connect to the MP server’s IP address and port, verify that the Adjacent Node configuration matches the association configuration at Main Menu > Transport Manager > Configuration > Transport.
- Contact My Oracle Support (MOS) for assistance if needed.

Table 117: RxTmSctpBufAvg

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>RxTmSctpBufAvg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Usage</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Average</td>
</tr>
</tbody>
</table>

Measurements
The Average Value of the number of bytes in SCTP RX Window

Collection Interval: 5 min

Peg Condition: Every Second, retrieve the Rx socket buffer occupancy by using the "getsockopt" functions and then calculates and peg the Average buffer occupancy, during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation.

Measurement Scope (Network, NE, Server): NE, Server

Customer Action: This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface

Table 118: RxTmSctpBufPeak

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>RxTmSctpBufPeak</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Usage</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Max</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The Peak Value of the number of bytes in SCTP RX Window.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>5 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>Every Second, retrieve the Rx socket buffer occupancy by using the &quot;getsockopt&quot; functions and then calculates and peg the Maximum buffer occupancy during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface</td>
</tr>
</tbody>
</table>

Table 119: TmSingleTransQueuePeak

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>TmSingleTransQueuePeak</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
</tbody>
</table>
**Measurement Type (Simple, Average, Min, Max, Duration)**
Max

**Measurement Description (255 chars)**
The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec).

**Collection Interval**
30 min

**Peg Condition**
Transport's Queue is registered as a Stack Resource, StackResourceManager thread monitors Peg Condition and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.

**Measurement Scope (Network, NE, Server)**
NE, Server

**Customer Action**
“Transport single queue utilization depicts the SCTP or UDP Transport Writer Queues utilization.”

This is a measure of how fast the Transport queue is being processed. It indicates the maximum depth of queue over the monitored interval. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist. Contact My Oracle Support (MOS) for assistance if needed.

---

**Table 120: TmSingleTransQueueAvg**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>TmSingleTransQueueAvg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Average</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The average single Transport (SCTP/UDP) Transport Writer Queue utilization (0-100%)</td>
</tr>
</tbody>
</table>
30 min Collection Interval

Transport’s Queue is registered as a Stack Resource, StackResourceManager thread monitors Peg Condition and updates the metric Average value for affected Transport.

NE, Server Measurement Scope (Network, NE, Server)

This is a measure of how fast the Transport queue is being processed. It indicates the Average depth of queue over the monitored interval.

Customer Action

It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist. Contact My Oracle Support (MOS) for assistance if needed.

Table 121: TmSingleTransQueueFull

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>TmSingleTransQueueFull</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The number of egress messages that were discarded because the single Transport Writer Queue was full.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>Check whether the single peers transmit data queue limit has reached its max limit (1000). If max limit is reached or exceeded then peg the measurement and discard the low priority events.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
</tbody>
</table>
This measurement indicates that the Transport is backed up and there could be messages that will get discarded. If it’s above the defined critical threshold, it results in generating an alarm. Contact *My Oracle Support (MOS).*

| Customer Action | This measurement indicates that the Transport is backed up and there could be messages that will get discarded. If it’s above the defined critical threshold, it results in generating an alarm. Contact *My Oracle Support (MOS).* |

Table 122: SctpTransPeerCWNDPeak

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>SctpTransPeerCWNDPeak</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Max</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option &quot;SCTP_STATUS&quot; through sctp_opt_info API.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>This is debug information, which is retrieved from sctp socket option (SCTP_STATUS). It indicates Peak of congestion window recorded for the peer address.</td>
</tr>
</tbody>
</table>

Table 123: SctpTransPeerCWNDAvg

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>SctpTransPeerCWNDAvg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Average</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
</tbody>
</table>
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

<table>
<thead>
<tr>
<th>Measurement Scope (Network, NE, Server)</th>
<th>NE, Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Action</td>
<td>This is debug information, which is retrieved from sctp socket option (SCTP_STATUS); It indicates Average of congestion window recorded for the peer address.</td>
</tr>
</tbody>
</table>

**Table 124: SctpTransPeerSRTTPeak**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>SctpTransPeerSRTTPeak</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Max</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option &quot;SCTP_STATUS&quot; through sctp_opt_info API.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).</td>
</tr>
</tbody>
</table>

**Table 125: SctpTransPeerSRTTAvg**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>SctpTransPeerSRTTAvg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Average</td>
</tr>
</tbody>
</table>
**Measurements**

<table>
<thead>
<tr>
<th>Measurement Description (255 chars)</th>
<th>The average value of smoothed round trip time for the SCTP Transport address during the collection interval.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option &quot;SCTP_STATUS&quot; through sctp_opt_info API.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Table 126: SctpTransUnAckedDataPeak</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Tag</td>
</tr>
<tr>
<td>Measurement Group (64 chars)</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
</tr>
<tr>
<td>Collection Interval</td>
</tr>
<tr>
<td>Peg Condition</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
</tr>
<tr>
<td>Customer Action</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Table 127: SctpTransUnAckedDataAvg</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Tag</td>
</tr>
<tr>
<td>Measurement Group (64 chars)</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
</tr>
</tbody>
</table>
### Table 128: SctpTransRTOPeak

<table>
<thead>
<tr>
<th>Measurement Description (255 chars)</th>
<th>The peak value of retransmission timeout in use for the SCTP Transport address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option &quot;SCTP_STATUS&quot; through sctp_opt_info API.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).</td>
</tr>
</tbody>
</table>

### Table 129: SctpTransRTOAvg

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>SctpTransRTOAvg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Performance</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Average</td>
</tr>
</tbody>
</table>

The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.

This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).
Measurements

<table>
<thead>
<tr>
<th>Measurement Description (255 chars)</th>
<th>The average value of retransmission timeout in use for the SCTP Transport address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option &quot;SCTP_STATUS&quot; through sctp_opt_info API.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).</td>
</tr>
</tbody>
</table>

Table 130: EvSctpAdjIPToDwn

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvSctpAdjIPToDwn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>Number of time configured IP Address of an Adjacent Node goes from Available to Unavailable.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• reachibility to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If all is well, this measurement should have a zero value. A non-zero value indicates a path fault to that address was detected. Troubleshooting:</td>
</tr>
<tr>
<td></td>
<td>• Check the event history log at Main Menu &gt; Alarms &amp; Events &gt; View History, looking for event 19410 - Adjacent Node IP Address state change. Event 19410 provides more details as to the actual cause of the failure.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at Main Menu &gt;</td>
</tr>
</tbody>
</table>
Transport Manager > Configuration > Adjacent Node.

- Verify the IP network connectivity between the MP server and the Adjacent Node’s IP address using a ping or traceroute command.
- Contact My Oracle Support (MOS) for assistance if needed.

### Table 131: EvSctpTransRej

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>EvSctpTransRej</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Group (64 chars)</td>
<td>Transport Exception</td>
</tr>
<tr>
<td>Measurement Dimension (Single, Arrayed)</td>
<td>Arrayed - per Transport</td>
</tr>
<tr>
<td>Measurement Type (Simple, Average, Min, Max, Duration)</td>
<td>Simple</td>
</tr>
<tr>
<td>Measurement Description (255 chars)</td>
<td>Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.</td>
</tr>
<tr>
<td>Collection Interval</td>
<td>30 min</td>
</tr>
<tr>
<td>Peg Condition</td>
<td>This measurement shall be incremented by one each time:</td>
</tr>
<tr>
<td></td>
<td>• the association has been rejected due to IP address validation failure in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.</td>
</tr>
<tr>
<td>Measurement Scope (Network, NE, Server)</td>
<td>NE, Server</td>
</tr>
<tr>
<td>Customer Action</td>
<td>If all is well, this measurement should have a zero value. A non-zero value indicates that the Adjacent Node has attempted to connect to the Peer IP Address at least once and but the connection attempt was rejected because the IP addresses advertised by the Adjacent Node failed validation. Troubleshooting:</td>
</tr>
<tr>
<td></td>
<td>• Transport status can be viewed at Main Menu &gt; Transport Manager &gt; Maintenance &gt; Transport.</td>
</tr>
<tr>
<td></td>
<td>• Check the event history log at Main Menu &gt; Alarms &amp; Events &gt; View History, looking for events 19411 - SCTP Transport closed due to failure of multihoming validation or 19412 - SCTP Transport Transport Configuration Mismatch. Events 19411 and/or 19412 provide more details as to the actual cause of the failure.</td>
</tr>
</tbody>
</table>
• Verify that the SCTP validation mode is as desired.
• Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at Main Menu > Transport Manager > Configuration > Adjacent Node.
• Verify that the remote port configured at Main Menu > Transport Manager > Configuration > Transport for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.
• Contact My Oracle Support (MOS) for assistance if needed.

### Transport Exception measurements

The Transport Exception measurement group contains measurements that provide information about exceptions and unexpected events related to the Transport Manager.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxTrFarEndClose</td>
<td>Number of times the far-end closed the association</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrManClose</td>
<td>Number of times the Transport was manually closed. This includes manual changes of the transport administrative state that cause the transport to transition from APP-UP to Disabled.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrNoRespClose</td>
<td>Number of times the Transport was closed due to lack of response from the far-end. This includes lack of response to any signaling sent on the transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrCnxFail</td>
<td>The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections.</td>
<td>30 min</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The number of times open attempt on UDP socket in Listen Mode failed on the Transport.</td>
<td></td>
</tr>
<tr>
<td>TxTrSendFail</td>
<td>The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxTrRcvFailed</td>
<td>The number of times an SCTP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvTrSockInitFail</td>
<td>Number of times the socket initialization failed</td>
<td>30 min</td>
</tr>
<tr>
<td>TmSingleTransQueueFull</td>
<td>The number of egress messages that were discarded because the singleTransport Writer Queue was full.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvSctpAdjIPToDwn</td>
<td>Number of time configured IP Address of an Adjacent Node goes from Available to Unavailable.</td>
<td>30 min</td>
</tr>
<tr>
<td>EvSctpTransRej</td>
<td>Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**RxTrFarEndClose**

- **Measurement Group:** Transport Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (per Transport)
- **Description:** The number of times the far end closed the SCTP connection
- **Collection Interval:** 30 min
- **Peg Condition:** Each time the far-end of the association closes the association by sending either SHUTDOWN or ABORT
- **Measurement Scope:** NE, Server
Recovery:

1. If the closing of the association was expected, no further action is necessary - the association will be recovered as soon as the far-end is ready to connect again.

2. If the closing of the association was not expected:
   a) Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
   b) Look in the event history at Main Menu > Alarms & Events > View History event 19404 - Far-end closed the Transport to determine exactly when the far-end closed the association.
   c) Look for other events for the association or MP server in the event history.
   d) Verify that IP connectivity still exists between the MP server and the SG.
   e) Verify whether the far-end of the association is undergoing maintenance.

EvTrManClose

Measurement Group: Transport Exception
Measurement Type: Simple
Measurement Dimension: Arrayed (per Transport)
Description: The number of times the Transport was manually closed. This includes manual changes of the transport administrative state that cause the transport to transition from APP-UP to Disabled.
Collection Interval: 30 min

Peg Condition Each time a manual change is made to the transport administrative state from Enabled to Blocked or from Enabled to Disabled, causing the transport to transition our of APP-UP protocol state.

Note: This condition has a special meaning for SS7/M3UA where it is linked with ASP-UP.
Measurement Scope: NE, Server

Recovery:

1. If the transport is known to be under maintenance, then no further action is necessary.

2. If the closing of the association was not expected:
   a) Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
   b) Look in the event history at Main Menu > Alarms & Events > View History event 19406 - Local Transport maintenance state change, which shows the manual transport state transitions and contains a time-stamp of when the change occurred.
   c) The security logs at Main Menu > Log Files > Security Logs History can be searched using the time-stamp from the event history log to determine which login performed the manual state change on the association.
   d) Contact My Oracle Support (MOS) for assistance if needed.

EvTrNoRespClose

Measurement Group: Transport Exception
Measurement Type: Simple
**Measurement Dimension:** Arrayed (per Transport)

**Description:** The number of times the transport was closed due to lack of response from the far end, including lack of response to any signaling sent on the transport.

**Collection Interval:** 30 min

**Peg Condition** Each time an established Transport is closed by the MP server due to lack of response at the SCTP level from the far-end of the association

**Measurement Scope:** NE, Server

**Recovery:**

1. If all is well, this measurement should have a zero value. If non-zero, the association has been closed due to lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the SG.

2. Otherwise:
   a) Transport status can be viewed at **Main Menu > Transport Manager > Maintenance > Transport**.
   b) Look in the event history at **Main Menu > Alarms & Events > View History** event 19405 - *Transport closed due to lack of response*.
   c) Verify IP connectivity between the MP server and the SG.
   d) Determine if the far-end of the association is congested, possibly causing slow response times on the association.
   e) Check the IP network between the MP server and the SG for excessive retransmissions.
   f) Contact **My Oracle Support (MOS)** for assistance if needed.

**EvTrCnxFail**

**Measurement Group:** Transport Exception

**Measurement Type:** Simple

**Measurement Dimension:** Arrayed (per Transport)

**Description:**

- The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections.
- The number of times open attempt on UDP socket in Listen Mode failed on the Transport.

**Collection Interval:** 30 min

**Peg Condition**

- Each time an SCTP connect attempt fails
- Each time an UDP open attempt in Listen mode fails
- Each time an SCTP open attempt in Listen mode fails

**Measurement Scope:** NE, Server

**Recovery:**
1. If all is well, this measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Peer IP Address at least once and failed to establish the SCTP connection.

2. Otherwise:
   a) Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
   b) Look in the event history at Main Menu > Alarms & Events > View History event 19402 - Failed to connect Transport, which provides more details as to the actual cause of the failure.
   c) Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at Main Menu > Transport Manager > Configuration > Adjacent Node.
   d) Verify that the remote port configured at Main Menu > Transport Manager > Configuration > Transport for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.
   e) Verify the IP network connectivity between the MP server and the Adjacent Node.
   f) If the SG must be configured to connect to the MP server's IP address and port, verify that the SG configuration matches the association configuration at Main Menu > Transport Manager > Configuration > Transport.
   g) Contact My Oracle Support (MOS) for assistance if needed.

### TxTrSendFail

**Measurement Group:** Transport Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.  
**Collection Interval:** 30 min  
**Peg Condition** Each time an attempt to send signaling DATA fails for any reason and the information being sent cannot be mapped to a specific transport  
**Measurement Scope:** NE, Server  

**Recovery:**

1. If all is well, this measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this Transport has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association.

2. Otherwise:
   a) Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
   b) Look in the event history at Main Menu > Alarms & Events > View History event 19407 - Failed to send Transport DATA Message, which gives more information about exactly what caused the failure to send.
   c) Verify that the IP network between the MP server and the Adjacent Node is functioning as expected.
   d) Contact My Oracle Support (MOS) for assistance if needed.
RxTrRecvFailed

**Measurement Group:** Transport Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.

**Collection Interval:** 30 min  
**Peg Condition:** Each time an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length.

**Measurement Scope:** NE, Server  
**Recovery:**

1. If all is well, this measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed.
2. Otherwise:
   a) Transport status can be viewed at **Main Menu > Transport Manager > Maintenance > Transport**.
   b) Look in the event history at **Main Menu > Alarms & Events > View History** event **19403 - Received malformed SCTP message (invalid length)**, which gives more information about exactly what caused the failure.
   c) Try to bring the sockets back into alignment by manually Disabling and Enabling the Transport.
   d) Contact **My Oracle Support (MOS)** for assistance if needed.

EvTrSockInitFail

**Measurement Group:** Transport Exception  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The number of times the socket initialization failed.

**Collection Interval:** 30 min  
**Peg Condition:** Each time one or more socket options cannot be set according to the settings in the transport’s configuration set.

**Measurement Scope:** NE, Server  
**Recovery:**

1. If all is well, this measurement should have a zero value. A non-zero value indicates some problem with association setup prior to attempting to connect the association.
2. If this issue occurs, look in **Main Menu > Alarms & Events > View History** for event **19401 - Failed to configure Transport**, which provides details about exactly what part of the configuration failed.
3. Contact **My Oracle Support (MOS)** for assistance if needed.
**TmSingleTransQueueFull**

- **Measurement Group:** Transport Exception
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (per Transport)
- **Description:** The number of egress messages that were discarded because the single Transport Writer Queue was full.
- **Collection Interval:** 30 min
- **Peg Condition** Check whether the single peers transmit data queue limit has reached its max limit (1000). If max limit is reached or exceeded then peg the measurement and discard the low priority events.
- **Measurement Scope:** NE, Server

**Recovery:**

1. This measurement indicates that the Transport is backed up and there could be messages that will get discarded. If it's above the defined critical threshold, it results in generating alarm 19408 - Single Transport Egress-Queue Utilization.
2. 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:

1. An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being received form the network.
2. The SCTP Association Writer process may be experiencing a problem preventing it from processing events from its event queue. The alarm log should be examined form Main Menu > Alarms & Events.
3. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. MP server status can be monitored form Main Menu > Status & Control > Server Status.
4. 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.
5. 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.

3. Contact My Oracle Support (MOS) for assistance if needed.

**EvSctpAdj**

- **Measurement Group:** Transport Exception
- **Measurement Type:** Max
**EvSctpTransRej**

**Measurement Group:** Transport Exception  
**Measurement Type:** Max  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.  
**Collection Interval:** 30 min  
**Peg Condition** Each time the association has been rejected due to IP address validation failure in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.  
**Measurement Scope:** NE, Server  
**Recovery:**  
1. If all is well, this measurement should have a zero value. A non-zero value indicates that the Adjacent Node has attempted to connect to the Peer IP Address at least once and but the connection attempt was rejected because the IP addresses advertised by the Adjacent Node failed validation.  
2. Otherwise:  
   1. Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.  
   2. Check the event history log at Main Menu > Alarms & Events > View History, looking for events 19411 - SCTP Transport closed due to failure of multihoming validation or 19412 - SCTP...
Transport Transport Configuration Mismatch which provide more details as to the actual cause of the failure.

3. Verify that the SCTP validation mode is as desired.
4. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct address at **Main Menu > Transport Manager > Configuration > Adjacent Node**.
5. Verify that the remote port configured at **Main Menu > Transport Manager > Configuration > Transport** for the association correctly identifies the port that the Adjacent node is listening on for SCTOp connections.
6. Contact *My Oracle Support (MOS)* for assistance if needed.

**Transport Usage measurements**

The Transport Usage measurement group contains measurements that provide information about the usage of the Transport Manager.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvTrCnxSuccess</td>
<td>The number of times the SCTP connection was successfully established on the Transport. The number of times the UDP socket in Listen Mode was opened successfully on the Transport.</td>
<td>30 min</td>
</tr>
<tr>
<td>TmTrEnaNotUp</td>
<td>The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxTmSctpBufAvg</td>
<td>The Average Value of the number of bytes in SCTP RX Window.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxTmSctpBufPeak</td>
<td>The Peak Value of the number of bytes in SCTP RX Window</td>
<td>5 min</td>
</tr>
</tbody>
</table>
EvTrCnxSuccess

**Measurement Group:** Transport Usage  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (per Transport)  

**Description:**  
- The number of times the SCTP connection was successfully established on the transport.  
- The number of times the UDP socket in Listen Mode was opened successfully on the Transport.  

**Collection Interval:** 30 min  

**Peg Condition:**  
- Each time the SCTP association reaches the APP-UP protocol state (i.e. the connection is successfully ESTABLISHED)  
- Each time the UDP socket in Listen Mode was opened successfully  

**Measurement Scope:** NE, Server  

**Recovery:**  
1. If the association is expected to have connected during the measurement reporting interval, no action is necessary.  
2. Otherwise:  
   a) Transport status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.  
   b) Look in the event history at Main Menu > Alarms & Events > View History events related to the association or the MP server to determine what may have caused the Transport to fail.  
   c) Contact My Oracle Support (MOS) for assistance if needed.

TmTrEnaNotUp

**Measurement Group:** Transport Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (per Transport)  

**Description:** The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.

**Collection Interval:** 30 min  

**Peg Condition** Time shall be accumulated for this measurement during the collection interval when all of the following are true:  
- the association is in the ENABLED administrative state  
- the association is not in the ASP-UP protocol state for M3UA and APP-UP for other Plugins.  

**Measurement Scope:** NE, Server
Recovery:

1. If all is well, this measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Peer IP Address at least once and failed to establish the SCTP connection.

2. Otherwise:
   a) Association status can be viewed at Main Menu > Transport Manager > Maintenance > Transport.
   b) Verify that the Adjacent Server that represents the far-end of the association is configured with the correct IP address at Main Menu > Transport Manager > Configuration > Adjacent Node.
   c) Verify that the remote port configured at Main Menu > Transport Manager > Configuration > Transport for the association correctly identifies the port that the SG is listening on for SCTP connections.
   d) Verify the IP network connectivity between the MP server and the SG.
   e) If the Adjacent Node must be configured to connect to the MP server’s IP address and port, verify that the Adjacent Node configuration matches the association configuration at Main Menu > Transport Manager > Configuration > Transport.
   f) Contact My Oracle Support (MOS) for assistance if needed.

RxTmSctpBufAvg

Measurement Group: Transport Usage
Measurement Type: Average
Measurement Dimension: Arrayed (per Transport)
Description: The Average Value of the number of bytes in SCTP RX Window
Collection Interval: 5 min
Peg Condition: Every Second, retrieve the Rx socket buffer occupancy by using the “getsockopt” functions and then calculates and peg the Average buffer occupancy, during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation.
Measurement Scope: NE, Server
Recovery:

No action required. This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface.

RxTmSctpBufPeak

Measurement Group: Transport Usage
Measurement Type: Max
Measurement Dimension: Arrayed (per Transport)
Description: The Peak Value of the number of bytes in SCTP RX Window
Collection Interval: 5 min
**Peg Condition** Every Second, retrieve the Rx socket buffer occupancy by using the "getsockopt" functions and then calculates and peg the Maximum buffer occupancy during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation.

**Measurement Scope:** NE, Server

**Recovery:**

No action required. This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface.

## Transport Performance measurements

The Transport Performance measurement group contains measurements that provide information about performance related measurements for the Transport Manager.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxTrOctets</td>
<td>The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
</tr>
<tr>
<td>RxTrOctets</td>
<td>The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.</td>
<td>30 min</td>
</tr>
<tr>
<td>TmSingleTransQueuePeak</td>
<td>The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval</td>
<td>30 min</td>
</tr>
<tr>
<td>TmSingleTransQueueAvg</td>
<td>The average single Transport Writer Queue utilization (0-100%) measured during the collection interval</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransPeerCWNDPeak</td>
<td>The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransPeerCWNDAvg</td>
<td>The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransPeerSRTTPeak</td>
<td>The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>SctpTransPeerSRRTAvg</td>
<td>The average value of smoothed round trip time for the SCTP Transport address during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransUnAckedDataPeak</td>
<td>The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransUnAckedDataAvg</td>
<td>The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransRTOPeak</td>
<td>The peak value of retransmission timeout in use for the SCTP Transport address</td>
<td>30 min</td>
</tr>
<tr>
<td>SctpTransRTOAvg</td>
<td>The average value of retransmission timeout in use for the SCTP Transport address</td>
<td>30 min</td>
</tr>
</tbody>
</table>

**TxTrOctets**

**Measurement Group:** Transport Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.  
**Collection Interval:** 30 min  
**Peg Condition** Each time a DATA/non-DATA message is successfully sent on the transport (incremented by the number of octets in the message).  
**Measurement Scope:** NE, Server  
**Recovery:**  
No action required. This measurement indicates the level of signaling octets that have been sent over the association during the reporting interval.

**RxTrOctets**

**Measurement Group:** Transport Performance  
**Measurement Type:** Simple
**Measurement Dimension:** Arrayed (per Transport)

**Description:** The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.

**Collection Interval:** 30 min

**Peg Condition** Each time a DATA/non-DATA message is successfully received on the transport (incremented by the number of octets in the message).

**Measurement Scope:** NE, Server

**Recovery:**

No action required. This measurement indicates the level of signaling octets that have been received over the association during the reporting interval.

---

**TmSingleTransQueuePeak**

**Measurement Group:** Transport Performance

**Measurement Type:** Max

**Measurement Dimension:** Arrayed (per Transport)

**Description:** The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec).

**Collection Interval:** 5 min

**Peg Condition** Transport's Queue is registered as a Stack Resource, StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.

**Measurement Scope:** NE, Server

**Recovery:**

1. Transport single queue utilization depicts the SCTP or UDP Transport Writer Queues utilization. This is a measure of how fast the Transport queue is being processed. It indicates the maximum depth of queue over the monitored interval. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
2. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
4. 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.

1. An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being received form the network.
2. 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.
3. 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.

4. 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.

5. 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.

5. Contact My Oracle Support (MOS) for assistance if needed.

### TmSingleTransQueueAvg

**Measurement Group:** Transport Performance  
**Measurement Type:** Average  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The average single Transport (SCTP/UDP) Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec).

**Collection Interval:** 30 min  
**Peg Condition:** Transport’s Queue is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport.

**Measurement Scope:** NE, Server  
**Recovery:**

1. This is a measure of how fast the Transport queue is being processed. It indicates the Average depth of queue over the monitored interval. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.

2. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

3. If the peak and average for an individual MP are significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist.

4. Contact My Oracle Support (MOS) for assistance if needed.

### SctpTransPeerCWNDPeak

**Measurement Group:** Transport Performance  
**Measurement Type:** Max  
**Measurement Dimension:** Arrayed (per Transport)  
**Description:** The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval.

**Collection Interval:** 30 min
Peg Condition This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope: NE, Server

Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS), It indicates Peak of congestion window recorded for the peer address.

SctpTransPeerCWNDAvg

Measurement Group: Transport Exception
Measurement Type: Average
Measurement Dimension: Arrayed (per Transport)
Description: The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.
Collection Interval: 30 min

Peg Condition This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope: NE, Server

Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS); It indicates Average of congestion window recorded for the peer address.

SctpTransPeerSRTTPeak

Measurement Group: Transport Performance
Measurement Type: Max
Measurement Dimension: Arrayed (per Transport)
Description: The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.
Collection Interval: 30 min

Peg Condition This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope: NE, Server

Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).
SctpTransPeerSRTTAvg

Measurement Group: Transport Performance
Measurement Type: Average
Measurement Dimension: Arrayed (per Transport)
Description: The average value of smoothed round trip time for the SCTP Transport address during the collection interval.
Collection Interval: 30 min
Peg Condition: This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope: NE, Server
Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransUnAckedDataPeak

Measurement Group: Transport Performance
Measurement Type: Max
Measurement Dimension: Arrayed (per Transport)
Description: The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.
Collection Interval: 30 min
Peg Condition: This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.
Measurement Scope: NE, Server
Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransUnAckedDataAvg

Measurement Group: Transport Performance
Measurement Type: Average
Measurement Dimension: Arrayed (per Transport)
Description: The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.
Collection Interval: 30 min
Peg Condition This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope: NE, Server
Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransRTOPeak

Measurement Group: Transport Performance
Measurement Type: Average
Measurement Dimension: Arrayed (per Transport)
Description: The peak value of retransmission timeout in use for the SCTP Transport address.
Collection Interval: 30 min

Peg Condition This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope: NE, Server
Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransRTOAvg

Measurement Group: Transport Performance
Measurement Type: Average
Measurement Dimension: Arrayed (per Transport)
Description: The average value of retransmission timeout in use for the SCTP Transport address.
Collection Interval: 30 min

Peg Condition This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope: NE, Server
Recovery:
This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).
**Topology Hiding Performance measurements**

The Topology Hiding Performance measurement report contains measurements providing information on the number of messages that the various topology hiding methods were applied.

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxPathTopology</td>
<td>Number of messages given path topology hiding treatment on messages routed to an Untrusted Network.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPathTopology</td>
<td>Number of messages given path topology hiding treatment on messages received from an Untrusted Network.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvHssTopology</td>
<td>Number of messages given S6a/S6d HSS topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMmeTopology</td>
<td>Number of messages given MME/SGSN topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMmeTopologyException</td>
<td>Number of messages given exception treatment while applying MME/SGSN topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvHssTopologyException</td>
<td>Number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>TxPathTopologyMp</td>
<td>Number of messages given path topology hiding treatment on messages routed to an Untrusted Network.</td>
<td>5 min</td>
</tr>
<tr>
<td>RxPathTopologyMp</td>
<td>Number of messages given path topology hiding treatment on messages received from an Untrusted Network.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvHssTopologyMp</td>
<td>Number of messages given S6a/S6d HSS topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMmeTopologyMp</td>
<td>Number of messages given MME/SGSN topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvMmeTopologyMpException</td>
<td>Number of messages given exception treatment while applying MME/SGSN topology hiding treatment.</td>
<td>5 min</td>
</tr>
<tr>
<td>EvHssTopologyMpException</td>
<td>Number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment.</td>
<td>5 min</td>
</tr>
</tbody>
</table>
TxPathTopology

**Measurement Group:** Topology Hiding Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Number of messages given path topology hiding treatment on messages routed to an Untrusted Network.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTH and ATH respectively.  
**Measurement Scope:** Site  
No action required

RxPathTopology

**Measurement Group:** Topology Hiding Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Number of messages given path topology hiding treatment on messages received from an Untrusted Network.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTR and ATR respectively.  
**Measurement Scope:** Site  
No action required

EvHssTopology

**Measurement Group:** Topology Hiding Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Number of messages given S6a/S6d HSS topology hiding treatment.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time S6a/S6d HSS TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR.  
**Note:** If S6a/S6d HSS TH treatment is applied to more than one AVP in a message, the counter is only incremented once.  
**Measurement Scope:** Site
No action required

**EvMmeTopology**

**Measurement Group:** Topology Hiding Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** Number of messages given MME/SGSN topology hiding treatment.  
**Collection Interval:** 5 min  
**Peg Condition:** Each time MME/SGSN TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR.  
**Note:** If MME/SGSN TH treatment is applied to more than one AVP in a message, the counter is only incremented once.  
**Measurement Scope:** Site  

No action required

**EvMmeTopologyException**

**Measurement Group:** Topology Hiding Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of messages given exception treatment while applying MME/SGSN topology hiding treatment.  
**Collection Interval:**  
**Peg Condition:** When MME/SGSN TH exception treatment is applied to either a Request or Answer message at RTH and ATH trigger points.  
**Recovery:**  
Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set

**EvHssTopologyException**

**Measurement Group:** Topology Hiding Performance  
**Measurement Type:** Simple  
**Measurement Dimension:** Arrayed (by Connection ID)  
**Description:** The number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment.  
**Collection Interval:**
Measurements

**Peg Condition:** When S6a/S6d HSS TH exception treatment is applied to Request at RTH trigger point.

**Recovery:**
Check with the HSS Vendor and request the vendor to be RFC 6733 Compliant.

**TxPathTopologyMp**

- **Measurement Group:** Topology Hiding Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of messages given path topology hiding treatment on messages routed to an Untrusted Network.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTH and ATH respectively.

**Measurement Scope:** Site
No action required

**RxPathTopologyMp**

- **Measurement Group:** Topology Hiding Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Single
- **Description:** Number of messages given path topology hiding treatment on messages received from an Untrusted Network.
- **Collection Interval:** 5 min
- **Peg Condition:** Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTR and ATR respectively.

**Measurement Scope:** Site
No action required

**EvHssTopologyMp**

- **Measurement Group:** Topology Hiding Performance
- **Measurement Type:** Simple
- **Measurement Dimension:** Arrayed (by Connection ID)
- **Description:** Number of messages given S6a/S6d HSS topology hiding treatment.
- **Collection Interval:** 5 min
Peg Condition: Each time S6a/S6d HSS TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR.

Note: If S6a/S6d HSS TH treatment is applied to more than one AVP in a message, the counter is only incremented once.

Measurement Scope: Site
No action required

EvMmeTopologyMp

Measurement Group: Topology Hiding Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: Number of messages given MME/SGSN topology hiding treatment.
Collection Interval: 5 min

Peg Condition: Each time MME/SGSN TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR.

Note: If MME/SGSN TH treatment is applied to more than one AVP in a message, the counter is only incremented once.

Measurement Scope: Site
No action required

EvMmeTopologyExceptionMp

Measurement Group: Topology Hiding Performance
Measurement Type: Simple
Measurement Dimension: Single
Description: The number of messages given exception treatment while applying MME/SGSN topology hiding treatment.

Collection Interval:

Peg Condition: When MME/SGSN TH exception treatment is applied to either a Request or Answer message at RTH and ATH trigger points.

Recovery:
Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set

EvHssTopologyExceptionMp

Measurement Group: Topology Hiding Performance
Measurement Type: Simple
**Measurement Dimension:** Single

**Description:** The number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment.

**Collection Interval:** 5 min

**Peg Condition:** When S6a/S6d HSS TH exception treatment is applied to Request at RTH trigger point.

**Recovery:**

Check with the HSS Vendor and request the vendor to be RFC 6733 Compliant.
Policy DRA Error Resolution Procedures

Topics:

- Error Code 500......961
- Error Code 501......961
- Error Code 502......962
- Error Code 2xx/3xx......963
- Error Code 510......963
- Error Code 511......964
- Error Code 512......964
- Error Code 513......965
- Error Code 503......966
- Error Code 505......967
- Error Code 507......968
- Error Code 508......968
- Error Code 520......969
- Error Code 521......969
- Error Code 504......970
- Error Code 509......971
- Error Code 305......971
- Error Code 305......972
- Error Code 522......972
- Error Code 523......973
- Error Code 525......973
- Error Code 506......974
- Error Code 530......975
- Error Code 531......975

This section provides information and procedures to help users diagnose and resolve internal error codes indexed by the Policy DRA application. These procedures are best used in combination with the Policy DRA Error Resolution section of the Policy DRA User’s Guide.
Error Code 500

**Associated Error Category:** Missing or Unconfigured APN

**Description:** Binding capable session initiation request is received with no APN.

**Associated P-DRA Alarm/Event:** 22730 - Policy DRA Configuration Error

**Associated Measurement:** RxBindCapMissingApn

**Associated Diameter Interface / Message Type:** Gx/Gxx CCR-I

**GUI Configurable:** Yes

**Recovery:**

1. See CCR-I Processing with PCRF Pool and findOrCreateBinding Response Processing with PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where this error occurs and the impacts on Gx/Gxx CCR signaling processing.

2. Go to the P-DRA GUI at Main Menu > Alarms & Events > View History. Set up the right scope for Server Group, Resource Domain, Place and Place Association, or use alarm 22730 - Policy DRA Configuration Error as Display Filter to start the search.

3. A list of alarm 22730 - Policy DRA Configuration Error should be displayed. Select an alarm based on the alarm time stamp or other preferred criteria that will bring in the details of the alarm in Main Menu > Alarms & Events > View History [Report].

4. Obtain the policy client's Origin-Host FQDN from the ERR_INFO in the alarm report on alarm 22730 - Policy DRA Configuration Error.

5. Go to Main Menu > Measurements > Report to obtain the measurement report for RxBindCapMissingApn and other relevant measurements. The frequency of the problem may be observed.

6. If needed, contact My Oracle Support (MOS) for further assistance.

---

Error Code 501

**Associated Error Category:** Missing or Unconfigured APN

**Description:** Binding capable session initiation request is received with an APN, but the APN is not configured in the APN configuration.

**Associated P-DRA Alarm/Event:** 22730 - Policy DRA Configuration Error

**Associated Measurement:** RxBindCapUnknownApn

**Associated Diameter Interface / Message Type:** Gx/Gxx CCR-I

**GUI Configurable:** Yes

**Recovery:**

1. See CCR-I Processing with PCRF Pool and findOrCreateBinding Response Processing with PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where this error occurs and the impacts on Gx/Gxx CCR signaling processing.
2. Go to the P-DRA GUI at **Main Menu > Alarms & Events > View History**. Set up the right scope for Server Group, Resource Domain, Place and Place Association, or use alarm **22730 - Policy DRA Configuration Error** as Display Filter to start the search.

3. A list of alarm **22730 - Policy DRA Configuration Error** should be displayed. Select an alarm based on the alarm time stamp or other preferred criteria that will bring in the details of the alarm in **Main Menu > Alarms & Events > View History [Report]**.

4. Obtain the policy client’s Origin-Host FQDN from the ERR_INFO in the alarm report on alarm **22730 - Policy DRA Configuration Error**.

5. If the APN string is expected, configure the APN at the NOAMP using **Main Menu > Policy DRA > Configuration > Access Point Names** screen.

6. If the APN string is not expected, it may imply that the policy client whose FQDN is specified in the ERR_INFO is using an invalid APN.

7. Go to **Main Menu > Measurements > Report** to obtain the measurement report for all relevant measurements. The frequency of the problem may be observed.

---

**Error Code 502**

**Associated Error Category:** Binding Found But Unable To Route  
**Description:** Request message is received and a binding with a PRCF was found. Policy DRA can’t route the request to PCRF due to DSR queue full error.

**Associated P-DRA Alarm/Event:** **22707 - Policy DRA Diameter Message Processing Failure**

**Associated Measurement:** **RxRequestMsgQueueFullDiscard**

**Associated Diameter Interface / Message Type:**
- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

**GUI Configurable:** Yes  
**Recovery:**

1. See *findSessionRef Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where this error occurs.

2. Go to the P-DRA NOAM GUI to collect information for possible root causes that may resort in the DRL queue being full:
   - Go to **Main Menu > Policy DRA > Status & Manage > Server** to verify is some DA-MPs have failed. If some servers on the same side fail, the traffic will be distributed amongst the remaining DA-MPs).
   - Go to **Main Menu > Status & Manage > KPIs** to check the ingress traffic rates of the DA-MPs. Each DA-MP in the site should have about the same ingress rate in normal situation.
   - Go to **Main Menu > Alarms & Events > View History** to search for relevant congestion alarms. The Display Filter may be set as Timestamp or Server to include P-DRA, DRL, or DCL alarms.

3. Go to **Main Menu > Measurements > Report** to obtain the measurement report for all relevant measurements.
Error Code 2xx/3xx

**Associated Error Category:** Binding Found But Unable To Route

**Description:** Request message is received and a binding with a PRCF was found. Policy DRA can’t route the request to PCRF due to PCRF being unreachable.

**Associated P-DRA Alarm/Event:** 22707 - Policy DRA Diameter Message Processing Failure

**Associated Measurement:** TxPdraAnswersGeneratedForDiameterErr

**Associated Diameter Interface / Message Type:**
- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

**GUI Configurable:** Yes

**Recovery:**
1. Error code 2xx/3xx is generated by DSR routing layer for various routing errors that result in the failure of routing the Diameter request to the PCRF.
2. Go to the P-DRA NOAM GUI to check the server status from **Main Menu > Policy DRA > Status & Manage > Server** to verify if some DA-MPs have failed (if some servers on the same side fail, the traffic will be distributed amongst the remaining DA-MPs).
3. Go to **Main Menu > Status & Manage > KPIs** to check the ingress traffic rates of the DA-MPs. Each DA- MP in the site should have about the same ingress rate in normal situation.
4. Go to **Main Menu > Alarms & Events > View History** to search for relevant congestion alarms. The Display Filter may be set as Timestamp or Server to include Policy DRA, DRL, or DCL alarms.
5. Check the Policy DRA SOAM GUI **Main Menu > Measurements > Report** to search for relevant measurements.

Error Code 510

**Associated Error Category:** Binding Found But Unable To Route

**Description:** A slave session could not be routed because, on polling the slave, sessionRef was no longer in the binding database.

**Associated P-DRA Alarm/Event:** N/A

**Associated Measurement:** PsbrSlavePollingFail

**Associated Diameter Interface / Message Type:**
- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

**GUI Configurable:** Yes
Recovery:

2. Go to the P-DRA SOAM GUI at Main Menu > Policy DRA > Status & Manage > Server to check binding pSBRs' status.
3. Go to the Main Menu > Alarms & Events > View History to check binding pSBR's congestion alarm/event info to determine a relation with the error.
4. Go to the Policy DRA SOAM GUI Main Menu > Measurements > Report to search for relevant measurements. Select, but not limited to, "pSBR Binding Exception" Measurement Group for the measurements directly related to this error.

Error Code 511

Associated Error Category: Binding Found But Unable To Route

Description: A slave session could not be routed because, on polling the master, sessionRef was no longer in the binding database.

Associated P-DRA Alarm/Event: N/A

Associated Measurement: PsbrSlavePollingFail

Associated Diameter Interface / Message Type:
- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. See Early binding Processing with PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Go to the P-DRA SOAM GUI at Main Menu > Status & Manage > Server to check binding pSBRs' status.
3. Get the measurement report from Main Menu > Measurements > Report to the frequency of the relevant measurements. Select, but not limited to, "pSBR Binding Exception" Measurement Group to determine the frequency of the relevant measurements.

Error Code 512

Associated Error Category: Binding Found But Unable To Route

Description: A slave session could not be routed because, on polling the master, sessionRef was early too long.

Associated P-DRA Alarm/Event: N/A
**Error Code 513**

**Associated Error Category:** Binding Found But Unable To Route

**Description:** A slave session could not be routed because, on polling the master, an internal error occurred.

**Associated P-DRA Alarm/Event:** N/A

**Associated Measurement:** PsbrSlavePollingFail

**Associated Diameter Interface / Message Type:**

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

**GUI Configurable:** Yes

**Recovery:**
1. Go to the P-DRA SOAM GUI at **Main Menu > Status & Manage > Server** to obtain the Policy DRA DA-MP and binding pSBR status.

2. Go to the **Main Menu > Alarms & Events > View History** to obtain the congestion alarm/event for Policy DRA DA-MP and/or binding pSBR, if congestion occurs. Some congestion conditions may be released after a short while. The error may not persist after the congestion condition is gone.

3. Go to Policy DRA SOAM GUI at **Main Menu > Communication Agent > Maintenance > Connection Status** to check the server connection status. The error may be caused by a disconnection between the local and peer nodes that the message was retransmitted the maximum number of times without receiving a response.

4. Get the measurement report from **Main Menu > Measurements > Report** for, but not limited to, "ComAgent Exception," "Connection Congestion," "pSBR Binding Exception" and 'Policy DRA Congestion' Measurement Groups.

### Error Code 503

**Associated Error Category:** No Usable Keys In Binding Dependent Message

**Description:** No binding key in Binding Key Priority GUI can be matched or no key is included in the binding dependent message.

**Associated P-DRA Alarm/Event:** 22706 - Binding Key Not Found In Diameter Message

**Associated Measurement:** TxPdraAnswersGeneratedForDiameterErr

**Associated Diameter Interface / Message Type:**
- Rx AAR
- Gx-Prime CCR-I

**GUI Configurable:** Yes

**Recovery:**

1. Check **AAR Processing** in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.

2. Go to Policy DRA NOAM GUI at **Main Menu > Policy DRA > Configuration > Binding Key Priority** to verify if the binding key priorities are expected (for instance IMSI and IPv56 Address are expected, but MSISDN and IPv4 are displayed instead).

3. If the binding key priorities are not expected, reset the binding key priority in this screen properly.

4. If the binding key priority are expected, check the validity of the received Request message as follows:
   - AVP carrying the expected key is present in the message
   - AVP carrying the expected key is correctly formed
   - AVP carrying the expected key is using a supported format (e.g. Subscription-ID AVP only Subscription-ID-Type of END_USER_E164 for MSISDN key and END_USER_IMSI for IMSI key).

5. Check the Policy DRA SOAM GUI at **Main Menu > Alarms & Events > View History** to search for all relevant alarms/events. The alarm Display Filter may be set as Timestamp to verify all alarms generated at the same time when the error occurred.

Error Code 505

Associated Error Category: Binding Not Found

Description: Binding record is not found after examining all configured binding keys in Diameter message.

Associated P-DRA Alarm/Event: 22718 - Binding Not Found for Binding Dependent Session Initiate Request

Associated Measurement: TxPdraAnswersGeneratedForPsbrErrResp

Associated Diameter Interface / Message Type:
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:
1. Check AAR Processing in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Go to Policy DRA NOAM GUI at Main Menu > Policy DRA > Configuration > Binding Key Priority to verify if the binding key priorities are expected (for instance IMSI and IPv56 Address are expected, but MSISDN and IPv4 are displayed instead).
3. If the binding key priorities are not expected, reset the binding key priority in this screen properly.
4. If the binding key priority are expected, check the validity of the received Request message as follows:
   - AVP carrying the expected key is present in the message
   - AVP carrying the expected key is correctly formed
   - AVP carrying the expected key is using a supported format (e.g. Subscription-ID AVP only Subscription-ID-Type of END_USER_E164 for MSISDN key and END_USER_IMSI for IMSI key).
5. Go to Policy DRA NOAM GUI at Main Menu > Policy DRA > Maintenance > Binding Key Query to query the IMSI key to find all alternate keys. If alternate records exist, compare the keys from the database to the keys in the request message to see if they match exactly (e.g. no extra digits or characters, etc.)
6. Check the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History to search for all relevant alarms/events. The alarm Display Filter may be set as Timestamp to verify all alarms generated at the same time when the error occurred.
Error Code 507

**Associated Error Category:** Policy SBR Error  
**Description:** Policy SBR Error - ComAgent timeout  
**Associated P-DRA Alarm/Event:** 22704 - Policy DRA Communication Agent Error  
**Associated Measurement:** TxPdraErrAnsGeneratedCAFailure  
**Associated Diameter Interface / Message Type:**  
- Gx CCR-I, CCR-U, and CCR-T  
- Rx AAR, STR  
- Gx-Prime CCR-I, CCR-U, and CCR-T  
**GUI Configurable:** Yes  
**Recovery:**  
1. Check `findSessionRef` Processing, `findOrCreateBindingResult` Processing, `findOrCreateBinding Response Processing with PCRF Pool`, `findSession Response Processing`, and `AAR Processing` in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.  
2. Go to Policy DRA SOAM GUI at Main Menu > Communication Agent > Maintenance > Connection Status to check the server connection status. The error may be caused by a disconnection between the local and peer nodes that the message was retransmitted the maximum number of times without receiving a response. Also check the Communication Agent Service status screen that corresponds to the ServiceID in the event instance to troubleshoot the operation of the service.  
4. Check the Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 19810 - Communication Agent Egress Message Discarded, 19811 - Communication Agent Ingress Message Discarded, 19814 - Communication Agent Peer has not responded to heartbeat, 19832 - Communication Agent Reliable Transaction Failed, 19833 - Communication Agent Service Egress Message Discarded, 22712 - Policy SBR Communication Error, 22722 - Policy DRA Binding Sub-resource Unavailable, and 22723 - Policy DRA Session Sub-resource Unavailable.

Error Code 508

**Associated Error Category:** Policy SBR Error  
**Description:** Policy SBR Error - pSBR database error prevents pSBR from reading, writing, or deleting a record  
**Associated P-DRA Alarm/Event:** 22711 - Policy SBR Database Error  
**Associated Measurement:** TxPdraAnswersGeneratedForPsbrErrResp  
**Associated Diameter Interface / Message Type:**
Policy DRA Error Resolution Procedures

- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: Yes

Recovery:

1. Check findSessionRef Processing, findOrCreateBindingResult Processing, findOrCreateBinding Response Processing with PCRF Pool, findSession Response Processing, and AAR Processing in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.

2. Go to Policy DRA NOAM GUI at Main Menu > Policy DRA > Maintenance > Policy SBR Status to verify the status of binding and session pSBR servers.

3. Check the Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22711 - Policy SBR Database Error). The table, operation, and key value of the pSBR DB where the error may occur will be indicated as well.

4. Get the measurement report from Main Menu > Measurements > Report for, but not limited to, "pSBR Binding Exception" and "pSBR Session Exception" Measurement Groups.

Error Code 520

Associated Error Category: Policy SBR Error

Description: Policy SBR PCRF Configuration Error - binding capable session initiation request received, but not PCRFs are configured at the site.

Associated P-DRA Alarm/Event: 22730 - Policy DRA Configuration Error

Associated Measurement: TxPdraAnswersGeneratedConfigErr

Associated Diameter Interface / Message Type: Gx CCR-I

GUI Configurable: Yes

Recovery:

1. Check findOrCreateBinding Response Processing with PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.

2. Check the Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22730 - Policy DRA Configuration Error).

3. If alarm 22730 - Policy DRA Configuration Error indicates that no PCRF are configured, configure PCRFs at the SOAM GUI at Main Menu > Policy DRA > Configuration > PCRFs.

Error Code 521

Associated Error Category: Policy SBR Error

Description: Policy SBR Error - maximum number of Sessions per Binding is Exceeded that fails the binding creation for given IMSI of MSISDN key.
Associated P-DRA Alarm/Event: 22719 - Maximum Number of Sessions per Binding Exceeded
Associated Measurement: TxPdraAnswersGeneratedForPsbrErrResp
Associated Diameter Interface / Message Type: Gx CCR-I, CCR-U, and CCR-T
GUI Configurable: Yes
Recovery:
1. Check findOrCreateBindingResult Processing and findOrCreateBinding Response Processing with PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Check the Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22719 - Maximum Number of Sessions per Binding Exceeded).
3. Go to Policy DRA NOAM GUI at Main Menu > Policy DRA > Maintenance > Binding Key Query by using event 22719 - Maximum Number of Sessions per Binding Exceeded to get all the information about session, including session-ids and PCEF FQDNs, to determine if the session is valid.
4. If the sessions exist in the Policy DRA, but not on the PCEF(s), contact My Oracle Support (MOS) for assistance.

Error Code 504

Associated Error Category: Policy SBR Error
Description: ComAgent resource unavailable when sending stack event to pSBR.
Associated P-DRA Alarm/Event: 22704 - Policy DRA Communication Agent Error
Associated Measurement: TxPdraErrAnsGeneratedCAFailure
Associated Diameter Interface / Message Type:
• Gx CCR-I, CCR-U, and CCR-T
• Rx AAR, STR
• Gx-Prime CCR-I, CCR-U, and CCR-T
GUI Configurable: Yes
Recovery:
1. Check CCR-I Processing with PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Check the Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 19810 - Communication Agent Egress Message Discarded, 19811 - Communication Agent Ingress Message Discarded, 19814 - Communication Agent Peer has not responded to heartbeat, 19832 - Communication Agent Reliable Transaction Failed, 19833 - Communication Agent Service Egress Message Discarded, and 22712 - Policy SBR Communication Error).
3. Check the Policy DRA SOAM GUI at Main Menu > Policy DRA > Maintenance > Policy SBR Status to verify the status of the binding pSBR, session pSBR, and related resources/sub-resources (Resource HA Role, Congestion Level, etc.)
4. Go to Main Menu > Communication Agent > Maintenance to verify Connection Status, Routed Services Status, and HA Services Status for resolving ComAgent unavailability.
Error Code 509

Associated Error Category: Session Not Found
Description: Session Not Found - session record doesn't exist for given session ID.
Associated P-DRA Alarm/Event: 22705 - Policy SBR Error Response Received By Policy DRA
Associated Measurement: PsbrFindSessDbErr
Associated Diameter Interface / Message Type:
• Gx CCR-I, CCR-U, and CCR-T
• Rx AAR, STR
• Gx-Prime CCR-I, CCR-U, and CCR-T
GUI Configurable: Yes
Recovery:
1. Check findSession Response Processing and AAR Processing in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Check the Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22716 - Policy SBR Audit Statistics Report to find the Session table to see if sessions were removed by audit.
3. Get the measurement report from Main Menu > Measurements > Report for, but not limited to, measurements PsbrExpiredSessionsFound, PsbrCreateSessDbErr, and PsbrRemSessRarAttempts.
4. Check if topology hiding applies to the policy client.
   Note: All checks may help to determine whether the session was never created, or was created, but removed by audit.

Error Code 305

Associated Error Category: Policy DRA Unavailable or Degraded
Description: Policy DRA Unavailable
Associated P-DRA Alarm/Event: 22500 - DSR Application Unavailable
Associated Measurement: RxApplUnavailableForRequest
Associated Diameter Interface / Message Type:
• All Gx requests
• All Rx Requests
• All Gx-Prime Requests
GUI Configurable: Yes
Recovery:
1. Go to the P-DRA SOAM GUI at Main Menu > Diameter > Maintenance > Applications to verify Policy DRA's admin state is set as expected.

2. Check the Main Menu > Diameter > Maintenance > Applications to verify Policy DRA's Operational Status and Congestion Level. Policy DRA's Operational Status is "Unavailable" when the operator has removed Policy DRA from service (Admin State is "Disabled").

3. Check Main Menu > Alarms & Events > View History for relevant events or alarms related to this DA-MP server.

4. Get the measurement report from Main Menu > Measurement > Report for, but not limited to, measurement RxApplUnavailableForAnswer.

Error Code 305

**Associated Error Category:** Policy DRA Unavailable or Degraded  
**Description:** Policy DRA Degraded  
**Associated P-DRA Alarm/Event:** 22501 - DSR Application Degraded  
**Associated Measurement:** RxApplUnavailableForRequest  
**Associated Diameter Interface / Message Type:**  
- All Gx requests  
- All Rx Requests  
- All Gx-Prime Requests  
**GUI Configurable:** Yes  
**Recovery:**  
1. Go to the P-DRA SOAM GUI at Main Menu > Diameter > Maintenance > Applications to verify Policy DRA's admin state is set as expected.  
2. Check the Main Menu > Diameter > Maintenance > Applications to verify Policy DRA's Operational Status and Congestion Level. Policy DRA's Operational Status is "Unavailable" when the operator has removed Policy DRA from service (Admin State is "Disabled").  
3. Check Main Menu > Alarms & Events > View History for relevant events or alarms related to this DA-MP server.  
4. Get the measurement report from Main Menu > Measurement > Report for, but not limited to, measurement RxApplUnavailableForAnswer.

Error Code 522

**Associated Error Category:** Session ID is missing from Request  
**Description:** Session ID is missing from Request  
**Associated P-DRA Alarm/Event:** 22700 - Protocol errors in Diameter Requests  
**Associated Measurement:** RxPdraRequestProtocolErr
Associated Diameter Interface / Message Type:

- All Gx requests
- All Rx Requests
- All Gx-Prime Requests

GUI Configurable: No (Result Code 5005)

Recovery:

1. Check Diameter Message Validation and CCR-I Processing without PCRF Pool in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22700 - Protocol errors in Diameter Requests).
3. Use the Origin-Host value of the received Request found in 22700 - Protocol errors in Diameter Requests to understand from where the Request was sent.

Error Code 523

Associated Error Category: CC-Request-Type AVP is missing from CCR message

Description: CC-Request-Type AVP is missing from CCR message

Associated P-DRA Alarm/Event: 22700 - Protocol errors in Diameter Requests

Associated Measurement: RxPdraRequestProtocolErr

Associated Diameter Interface / Message Type: Gx CCR-I, CCR-U, and CCR-T

GUI Configurable: No (Result Code 5005)

Recovery:

1. Check CCR Processing in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22700 - Protocol errors in Diameter Requests).
3. Use the Origin-Host value of the received Request found in 22700 - Protocol errors in Diameter Requests to understand from where the Request was sent.

Error Code 525

Associated Error Category: Invalid AVP value in request message
Description: Invalid AVP value in request message

Associated P-DRA Alarm/Event: 22700 - Protocol errors in Diameter Requests

Associated Measurement: RxPdraRequestProtocolErr

Associated Diameter Interface / Message Type:
- All Gx requests
- All Rx Request
- All Gx-Prime Requests

GUI Configurable: No (Result Code 5004)

Recovery:
1. Check CCR Processing in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22700 - Protocol errors in Diameter Requests).
3. Use the Origin-Host value of the received Request found in 22700 - Protocol errors in Diameter Requests to understand from where the Request was sent.

Error Code 506

Associated Error Category: Destination-Host AVP is missing in in-session request

Description: Destination-Host AVP is missing in in-session request

Associated P-DRA Alarm/Event: 22700 - Protocol errors in Diameter Requests

Associated Measurement: RxPdraRequestProtocolErr

Associated Diameter Interface / Message Type:
- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: No (Result Code 5012)

Recovery:
1. Check STR Processing and ASR/ASA Processing in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22700 - Protocol errors in Diameter Requests).
3. Use the Origin-Host value of the received Request found in 22700 - Protocol errors in Diameter Requests to understand from where the Request was sent.

**Error Code 530**

Associated Error Category: Unsupported Application ID  
Description: Application ID unsupported by Policy DRA  
Associated P-DRA Alarm/Event: 22700 - Protocol errors in Diameter Requests  
Associated Measurement: RxPdraRequestProtocolErr  
Associated Diameter Interface / Message Type: Diameter Requests  
GUI Configurable: No (Result Code 3007)  
Recovery:  
1. Check Diameter Message Validation in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.  
2. Go to the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22700 - Protocol errors in Diameter Requests ).  
3. Use the Origin-Host value of the received Request found in 22700 - Protocol errors in Diameter Requests to understand from where the Request was sent.  

**Error Code 531**

Associated Error Category: Command Code and App ID no match  
Description: Command Code doesn't match the App ID or doesn't exist  
Associated P-DRA Alarm/Event: 22700 - Protocol errors in Diameter Requests  
Associated Measurement: RxPdraRequestProtocolErr  
Associated Diameter Interface / Message Type: Diameter Requests  
GUI Configurable: No (Result Code 5019)  
Recovery:  
1. Check Diameter Message Validation in the Error Resolution appendix of the Policy DRA User Guide to investigate and understand the circumstances where the error occurs.  
2. Go to the Policy DRA SOAM GUI at Main Menu > Alarms & Events > View History and set the Display Filter by Event-IDs (in particular, 22700 - Protocol errors in Diameter Requests ).  
3. Use the Origin-Host value of the received Request found in 22700 - Protocol errors in Diameter Requests to understand from where the Request was sent.
AAR | Authentication, Authorization Request (Rx Diameter command)

ACK | Data Acknowledgement

ANSI | American National Standards Institute
An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.

APN | Access Point Name
The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.

ASP | Abstract Service Primitive
Application Server Process
A process instance of an Application Server. An Application Server Process serves as an active or standby process of an Application Server (e.g., part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances of) MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP end-point,
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>and may be configured to process signaling traffic within more than one Application Server.</td>
</tr>
<tr>
<td>ASR</td>
<td>Abort-Session-Request</td>
</tr>
<tr>
<td>Association</td>
<td>An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.</td>
</tr>
<tr>
<td>ATH</td>
<td>Application Trouble Handler</td>
</tr>
<tr>
<td>ATR</td>
<td>Application-terminated routing</td>
</tr>
<tr>
<td>ATR</td>
<td>Routing rule that operates on outgoing application-terminated (AT) messages.</td>
</tr>
<tr>
<td>ATR</td>
<td>Answer Topology Restoral (DSR)</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute-Value Pair</td>
</tr>
<tr>
<td>AVP</td>
<td>The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input-Output System</td>
</tr>
<tr>
<td>BIOS</td>
<td>Firmware on the CPU blade that is executed prior to executing an OS.</td>
</tr>
</tbody>
</table>
**Glossary**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CAPM</strong></td>
<td>Computer-aided policy making</td>
</tr>
</tbody>
</table>
| **CCA** | Credit Control Answer  
The Diameter message that is received from the prepaid rating engine to acknowledge a CCR command. |
| **CCR** | Continuity Check Request  
Credit Control Request  
A Diameter message to be sent to a prepaid rating engine to request credit authorization for an SMS. |
| **CCR-I** | CCR Initial |
| **CdPA** | Called Party Address - The field in the SCCP portion of the MSU that contains the additional addressing information of the destination of the MSU. Gateway screening uses this additional information to determine if MSUs that contain the DPC in the routing label and the subsystem number in the called party address portion of the MSU are allowed in the network where the EAGLE is located. |
| **CEA** | Capability-Exchange-Answer  
The Diameter response that the prepaid rating engine sends to the Mobile Originated application during capability exchanges. |
| **CER** | Capabilities-Exchange-Request  
A Diameter message that the Mobile Originated application sends to a prepaid rating engine to perform a capability exchange. The |
C

CER (indicated by the Command-Code set to 257 and the Command Flags ‘R’ bit set) is sent to exchange local capabilities. The prepaid rating engine responds with a Capability-Exchange-Answer (CEA) message.

Charging Proxy Application

A DSR Application that is responsible for sending and receiving Diameter accounting messages.

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.

COMCOL

Communications Core Object Library

A suite of re-usable C++ libraries, as well as processes and procedures available for use in Tekelec products. Many of its features are focused toward the communications area of software developments, although it purpose
is not intended to restrict its functionality to any particular area

Communication Agent
See ComAgent.

CPA
Capability Point Code ANSI Charging Proxy Application
The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.

CPC
Capability Point Code
A capability point code used by the SS7 protocol to identify a group of 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).

DA-MP
Diameter Agent Message Processor
A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that
is hosting a Diameter Signaling Router Application.

**DAVA**
Destination Available

**DB**
Database
Daughter Board
Documentation Bulletin
Data bus

**DCL**
Diameter Connection Layer
The software layer of the stack which implements Diameter transport connections.

**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 mobility management which is typically associated with an IMS or wireless type of environment.

**DIH**
Diameter Intelligence Hub
A troubleshooting solution for LTE, IMS, and 3G Diameter traffic processed by the DSR. DIH does not require separate probes or taps.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM-IWF</td>
<td>Diameter–MAP Interworking DSR Application, which translates Diameter messages into MAP messages</td>
</tr>
</tbody>
</table>
| DNS          | Domain Name Services  
A system for converting Internet host and domain names into IP addresses. |
| DP           | Data Processor  
The repository of subscriber data on the individual DSR node elements. The DP hosts the full address resolution database. |
| DPA          | Disconnect-Peer-Answer  
A message used by a Diameter node to answer the Disconnect-Peer-Request (DPR). |
| 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. |
| DRST         | Destination Restricted |
| DSR          | Data Set Ready |
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 may consist of one or more Diameter nodes.

Delete Subscriber Data Request

DUNA
Destination Unavailable

DUPU
Destination User Part Unavailable
An M3UA management message.

Device-Watchdog-Answer
A Diameter message used with the Device-Watchdog-Request (DWR) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the prepaid rating engine within the configured timeout period, a DWR message is sent to the prepaid rating engine. If the prepaid rating engine fails to respond with a DWA within the required time, the connection is closed with the prepaid rating engine and initiates failover procedures. All new and pending requests are then sent to the secondary server.

Device-Watchdog-Request
A Diameter message used with the Device-Watchdog-Answer (DWA) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application
and the Diameter server within the configured timeout period, a DWR message is sent to the Diameter Server. If the Diameter server fails to respond within the required time, the connection is closed with the Diameter server and initiates failover procedures. All new and pending requests are then sent to the secondary Diameter server.

**Glossary**

**D**

Egress Message Rate

**E**

**EMR**

Egress Message Rate

**EPT**

Egress Pending Transaction. The number of transactions pending for answers on a connection or peer (or a group of connections/peers)

**ETG**

Egress Throttle Group (s)

**ETG-PCL**

Egress Throttle Group Pending Transaction Limiting Congestion Level. ETG-PCL of 0 denotes that state of Rate Limiting function is Normal. ETG-PCL of X (X > 0) denotes that Requests of Priority less than X will not be allowed to send to Peers or Diameter Connections in that ETG.

**ETG-RCL**

Egress Throttle Group - Rate Limiting Congestion Level. ETG-RCL of 0 denotes that state of Rate Limiting function is Normal. ETG-RCL of X (X > 0) denotes that Requests of Priority less than X will not be allowed to send to Peers or Diameter Connections in that ETG.

**F**

Full Address Based Resolution
F

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.

Full Address Based Resolution

See FABR.

G

GGA

Get-Gateway-Answer A reply to a GGR. It contains session information for the subscriber present in the GGR. GGA includes the bindings for the subscriber such as, Access Point Name, PCEF FQDN and Creation timestamp. The session information is aggregated in the GGA based on the PCRF to which is it assigned.

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 query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA
G

processes Diameter Requests and generates Diameter Answers.

GQC

Gateway Query Client also known as Diameter Node

GT

Global Title Routing Indicator

GTI

Global Title Indicator

GUI

Graphical User Interface
The term given to that set of items and facilities which provide the user 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.

Gx

The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.
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.

HP

Hewlett-Packard

HSS

Home Subscriber Server
A central database for subscriber information.

IDIH

Integrated Diameter Intelligence Hub

IMSI

International Mobile Subscriber Identity
A unique internal network ID identifying a mobile subscriber.

IMR

Ingress Message Rate

IP

Intelligent Peripheral
Internet Protocol
IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
### Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| ITU | International Telecommunications Union  
An organization that operates worldwide to allow governments and the private telecommunications sector to coordinate the deployment and operating of telecommunications networks and services. The ITU is responsible for regulating, coordinating and developing international telecommunications, and for harmonizing national political interests. |
| IWF | InterWorking Function |
| KPI | Key Performance Indicator |
| 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. |
| M3RL | M3UA Routing Layer |
### M
A layer invented by Tekelec to enhance M3UA by adding a true routing layer.

### MAP
Mated Application Part
Mobile Application Part
An application part in SS7 signaling for mobile communications systems.

### MD-IWF
MAP-Diameter Interworking SS7 Application, which translates MAP messages into Diameter messages

### Message Processor
See MP

### MME
Mobility Management Entity

### 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&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

### MSISDN
Mobile Station International Subscriber Directory Number
The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.

Mobile Subscriber Integrated Services Digital Network [Number]
M

Mobile Station International Subscriber Directory Number. The unique, network-specific subscriber number of a mobile communications subscriber. MSISDN follows the E.164 numbering plan; that is, normally the MSISDN is the phone number that is used to reach the subscriber.

MTP

Message Transfer Part

The levels 1, 2, and 3 of the SS7 protocol that control all the functions necessary to route an SS7 MSU through the network.

Module Test Plan

N

NE

Network Element

An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location.

In a 2-Tiered DSR OAM system, this includes the NOAM and all MPs underneath it. In a 3-Tiered DSR OAM system, this includes the NOAM, the SOAM, and all MPs associated with the SOAM.

Network Entity

NI

Network Indicator

NTP

Network Time Protocol

NTP daemon

Network Time Protocol daemon – NTP process that runs in the background.
O

OAM
Operations, Administration, and Maintenance
The application that operates the Maintenance and Administration Subsystem which controls the operation of many products.

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
Originating Point Code
Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.

P

PCRF
Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network.
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
P
anywhere in the network, must be processed by the same PCRF.

P-DRA
Policy DRA

PDU
Protocol Data Unit

Peer
A Diameter node to which a given Diameter node has a direct transport connection.

pSBR
Policy SBR

PTR
Pending Transaction Record

R

Range Based Address Resolution
See RBAR.

RAR
Re-Authorization Request (Gx or Rx Diameter command)

RBAR
Range Based Address Resolution
A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, “Routing Entity” Type, and Routing Entity address ranges.

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
R

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.

<table>
<thead>
<tr>
<th>REPL</th>
<th>Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>RI</td>
<td>Routing Indicator</td>
</tr>
<tr>
<td>RSP</td>
<td>Route Set Test - Prohibited message</td>
</tr>
<tr>
<td></td>
<td>Remote Signaling Point</td>
</tr>
<tr>
<td></td>
<td>Represents an SS7 network node (point code) that signaling must be sent to. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.</td>
</tr>
<tr>
<td></td>
<td>Remote Signaling Point</td>
</tr>
<tr>
<td></td>
<td>A logical element that represents a unique point code within a particular SS7 domain with which the SS7 application’s Local Signaling Point interacts.</td>
</tr>
<tr>
<td>RTH</td>
<td>Request Topology Hiding - A Topology Hiding trigger point that identifies a location within Diameter routing where topology-related information in a Request message is hidden or obscured based upon a set of Topology Hiding rules.</td>
</tr>
<tr>
<td>RTR</td>
<td>Router</td>
</tr>
<tr>
<td></td>
<td>Routes all types of SMS traffic.</td>
</tr>
<tr>
<td></td>
<td>Request Topology Restoral</td>
</tr>
</tbody>
</table>
SBR
Subsystem Backup Routing
Session Binding Repository - A highly available, distributed database for storing Diameter session binding data.

SCCP
Signaling Connection Control Part
The signaling connection control part with additional functions for the Message Transfer Part (MTP) in SS7 signaling. Messages can be transmitted between arbitrary nodes in the signaling network using a connection-oriented or connectionless approach.

SCON
Signaling Congested

SCTP
Stream Control Transmission Protocol
An IETF transport layer protocol, similar to TCP that sends a message in one operation.
The transport layer for all standard IETF-SIGTRAN protocols.
SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

Session Binding Repository
See SBR.

SG
Secure Gateway
Signaling Gateway
S

A network element that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be coresident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (e.g., signaling backhaul). A Signaling Gateway could be modeled as one or more Signaling Gateway Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers.

SGSN

Serving GPRS Support Node

SNMP


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
Site Operations, Administration, and Maintenance
S

SOAP
Simple Object Access Protocol

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.
Spanning Tree Protocol

STR
Send_to_Resource AIN message
Session Termination Request (Rx Diameter command)

SW
Software
Switch

T

TFA
TransFer Allowed (Msg)

TFC
Transfer Control
TransFer Controlled (Msg)
Transfer Congested

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

TH
Topology Hiding
Glossary

T

TPC
True Point Code

TTR
Team Test Ready
Triggerless TCAP Relay
Trace Transaction Record - A record describing a Diameter transaction, including all of the Diameter messages that were part of the transaction, plus the operations performed by DSR while processing those messages.

U

Untrusted Network
A Diameter network which has topology information hidden by the Topology Hiding features.

X

XUDT
Extended Unit Data
Extended User Data