

**Oracle® Communications
Tekelec HLR Router**

HLR Router Alarms, KPIs, and Measurements Reference

E72253 Revision 01

June 2016

Tekelec HLR Router HLR Router Alarms, KPIs, and Measurements Reference

Copyright © 2014, 2016, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

Table of Contents

Chapter 1: Introduction.....	23
Overview.....	24
Scope and Audience.....	24
Manuel Organization.....	24
Documentation Admonishments.....	25
Related Publications.....	25
Locate Product Documentation on the Oracle Help Center Site.....	26
Customer Training.....	26
My Oracle Support (MOS).....	27
Emergency Response.....	27
Chapter 2: Alarms and Events, KPIs, and Measurements	
Overview.....	28
Displaying the file list.....	29
Opening a file.....	29
Data Export.....	29
Data Export elements.....	29
Configuring data export.....	31
Tasks.....	32
Active Tasks.....	32
Scheduled Tasks.....	36
Chapter 3: Alarms and Events.....	38
General alarms and events information.....	39
Alarms and events overview.....	39
Alarms formatting information.....	40
Alarm and event ID ranges.....	41
Alarm and event types.....	41
Viewing active alarms.....	43
Active alarms data export elements.....	43
Exporting active alarms.....	44
Generating a report of active alarms.....	45

Viewing alarm and event history.....	46
Historical events data export elements.....	46
Exporting alarm and event history.....	47
Generating a report of historical alarms and events.....	48
Security Log View History elements.....	49
Viewing security log files.....	49
Security log data export elements.....	50
Exporting security log files.....	50
Generating a Security Log report.....	52
OAM (10000-10999).....	52
10000 - Incompatible database version.....	52
10001 - Database backup started.....	52
10002 - Database backup completed.....	53
10003 - Database backup failed.....	53
10004 - Database restoration started.....	53
10005 - Database restoration completed.....	54
10006 - Database restoration failed.....	54
10008 - Database provisioning manually disabled	54
10009 - Config and Prov db not yet synchronized	55
10010 - Stateful db from mate not yet synchronized.....	55
10011 - Cannot monitor table.....	55
10012 - Table change responder failed	56
10013 - Application restart in progress	56
10020 - Backup failure	56
10050 - Resource Audit Failure.....	57
10051 - Route Deployment Failed.....	57
10052 - Route discovery failed.....	57
10053 - Route deployment failed - no available device.....	58
10054 - Device deployment failed.....	58
10055 - Device discovery failed.....	58
10073 - Server Group Max Allowed HA Role Warning.....	59
10074 - Standby server degraded while mate server stabilizes.....	59
10075 - Application processes have been manually stopped.....	60
10078 - Application not restarted on standby server due to disabled failure cleanup mode.....	60
10100 - Log export started.....	60
10101 - Log export successful.....	61
10102 - Log export failed.....	61
10103 - Log export already in progress.....	61
10104 - Log export file transfer failed.....	62
10105 - Log export cancelled - user request.....	62

10106 - Log export cancelled - duplicate request.....	63
10107 - Log export cancelled - queue full.....	63
10108 - Duplicate scheduled log export task.....	63
10109 - Log export queue is full.....	64
10110 - Certificate About to Expire.....	64
10111 - Certificate Expired.....	65
10112 - Certificate Cannot Be Used.....	65
10115 - Health Check Started.....	65
10116 - Health Check Successful.....	66
10117 - Health Check Failed.....	66
10118 - Health Check Not Run.....	66
10120 - Server Group Upgrade Started.....	67
10121 - Server Group Upgrade Cancelled - Validation Failed.....	67
10122 - Server Group Upgrade Successful.....	67
10123 - Server Group Upgrade Failed.....	68
10124 - Server Group Upgrade Cancelled - User Request.....	68
10130 - Server Upgrade Started.....	68
10131 - Server Upgrade Cancelled.....	69
10132 - Server Upgrade Successful.....	69
10133 - Server Upgrade Failed.....	69
10134 - Server Upgrade Failed.....	70
10151 - Login successful.....	70
10152 - Login failed.....	71
10153 - Logout successful.....	71
10154 - User Account Disabled.....	71
10155 - SAML Login Successful.....	72
10156 - SAML Login Failed.....	72
10200 - Remote database reinitialization in progress.....	72
HLR Alarms (14000-14999).....	73
14100 - PDB interface disabled.....	73
14101 - No remote client connections.....	73
14102 - PDBI Connection failed.....	74
14120 - PDBI Connection established.....	74
14121 - PDBI Connection terminated.....	74
14122 - PDBI connection denied.....	75
14140 - PDB import throttled.....	75
14150 - PDB import initialization failed.....	76
14151 - PDB import generation failed.....	76
14152 - PDB import transfer failed.....	77
14153 - PDB export initialization failed.....	77
14154 - PDB export generation failed.....	78

14155 - PDB export transfer failed.....	78
14160 - PDBI Import successful.....	79
14161 - PDBI Export successful.....	79
14170 - EPAP Audit started and in progress.....	80
14171 - EPAP Audit aborted.....	80
14172 - EPAP Audit failed to complete.....	80
14173 - EPAP Audit completed.....	81
14174 - NPA Split activation failed.....	81
14175 - NPA Split started and is active.....	81
14176 - NPA Split completion failed.....	82
14177 - NPA Split completed.....	82
14178 - NPA Split completed.....	82
14200 - Failed to initialize PDE task.....	83
14201 - PDE failed to collect performance data.....	83
14202 - PDE failed to generate report in CSV format.....	83
14203 - PDE failed to transfer CSV file.....	84
14210 - Failed to initialize Key Exchange for PDE.....	84
14211 - Failed to exchange keys for PDE.....	84
14212 - Failed to delete password from PDE Options table.....	85
14230 - PDE successful.....	85
14231 - PDE Key Exchange successful.....	86
14301 - ERA Responder failed.....	86
14400 - Default value not configured in ExhrOptions table.....	86
14401 - Service config entry not configured.....	87
14402 - Number trans entry not configured.....	87
14403 - Exception entry not configured.....	88
14405 - Invalid CdPA GTI.....	88
14406 - Cannot route to Network Entity.....	88
14407 - Mate not configured.....	89
14408 - MP E164 Not Configured.....	89
SS7/Sigtran Alarms (19200-19299).....	90
19200 - RSP/Destination unavailable.....	90
19201 - RSP/Destination route unavailable.....	90
19202 - Linkset unavailable.....	91
19203 - Link unavailable.....	91
19204 - Preferred route unavailable.....	92
19205 - TFP received.....	92
19206 - TFA received.....	93
19207 - TFR received.....	93
19208 - TFC received.....	93
19209 - M3RL routing error.....	94

19210 - M3RL routing error - invalid NI.....	94
19211 - M3RL routing error - invalid SI.....	95
19212 - CFG-DB Validation Error.....	96
19213 - CFG-DB Update Failure.....	96
19214 - CFG-DB post-update Error.....	97
19215 - CFG-DB post-update Failure.....	97
19216 - Measurement Initialization Failure.....	98
19217 - Node isolated - all links down.....	98
19226 - Timedout waiting for ASP-UP-ACK.....	98
19227 - Received unsolicited ASP-DOWN-ACK.....	99
19229 - Timed out waiting for ASP-ACTIVE-ACK.....	99
19230 - Received unsolicited ASP-INACTIVE-ACK.....	100
19231 - Received invalid M3UA message.....	100
19233 - Failed to send non-DATA message.....	101
19234 - Local link maintenance state change.....	102
19235 - Received M3UA error.....	102
19240 - Remote SCCP subsystem prohibited.....	103
19241 - SCCP malformed or unsupported message.....	104
19242 - SCCP Hop counter violation.....	104
19243 - SCCP routing failure.....	105
19244 - SCCP routing failure network status.....	105
19245 - SCCP GTT failure.....	106
19246 - Local SCCP subsystem prohibited.....	106
19248 - SCCP Segmentation Failure.....	107
19249 - SCCP Reassembly Failure.....	108
19250 - SS7 process CPU utilization.....	108
19251 - Ingress message rate.....	109
19252 - PDU buffer pool utilization.....	109
19253 - SCCP stack event queue utilization.....	110
19254 - M3RL stack event queue utilization.....	110
19255 - M3RL network management event queue utilization.....	111
19256 - M3UA stack event queue utilization.....	112
19258 - SCTP Aggregate Egress queue utilization.....	112
19259 - Operation discarded due to local resource limitation.....	113
19260 - Transaction could not be delivered to remote TCAP peer due to conditions in the network.....	113
19262 - Operation discarded due to malformed component received from remote TCAP peer.....	114
19263 - Transaction discarded due to malformed dialogue message received from local TC User.....	114

19264 - Transaction discarded due to malformed dialogue message from remote TCAP peer.....	115
19265 - Unexpected event received from local TC User.....	115
19266 - Unexpected event received from remote TCAP peer.....	116
19267 - Dialogue removed by dialogue cleanup timer.....	116
19268 - Operation removed by invocation timer expiry.....	117
19269 - Dialogue aborted by remote TCAP peer.....	117
19270 - Received unsupported TCAP message.....	118
19271 - Operation rejected by remote TCAP peer.....	118
19272 - TCAP active dialogue utilization.....	119
19273 - TCAP active operation utilization.....	119
19274 - TCAP stack event queue utilization.....	120
19275 - Return error from remote TCAP peer.....	121
Transport Manager Alarms and Events (19400-19499).....	121
19400 - Transport Down.....	121
19401 - Failed to configure Transport.....	122
19402 - Failed to connect Transport.....	123
19403 - Received malformed SCTP message (invalid length).....	123
19404 - Far-end closed the Transport.....	124
19405 - Transport closed due to lack of response.....	124
19406 - Local Transport maintenance state change.....	125
19407 - Failed to send Transport DATA Message.....	125
19408 - Single Transport Egress-Queue Utilization.....	126
19409 - Message Rejected by ACL Filtering.....	127
19410 - Adjacent Node IP Address state change.....	127
19411 - SCTP Transport closed due to failure of multihoming validation.....	128
19412 - SCTP Transport configuration mismatched for Adjacent Node IP.....	128
19413 - SCTP Transport closed due to unsupported peer address event recieved.....	128
Communication Agent, ComAgent (19800-19909).....	129
19800 - Communication Agent Connection Down.....	129
19801 - Communication Agent Connection Locally Blocked.....	130
19802 - Communication Agent Connection Remotely Blocked.....	131
19803 - Communication Agent stack event queue utilization.....	131
19804 - Communication Agent configured connection waiting for remote client to establish connection.....	132
19805 - Communication Agent Failed To Align Connection.....	133
19806 - Communication Agent CommMessage mempool utilization.....	134
19807 - Communication Agent User Data FIFO Queue utilization.....	135
19808 - Communication Agent Connection FIFO Queue utilization.....	136
19810 - Communication Agent Egress Message Discarded.....	137
19811 - Communication Agent Ingress Message Discarded.....	137

19814 - Communication Agent Peer has not responded to heartbeat.....	138
19816 - Communication Agent Connection State Changed.....	138
19817 - Communication Agent DB Responder detected a change in configurable control option parameter.....	139
19818 - Communication Agent DataEvent Mempool utilization.....	139
19820 - Communication Agent Routed Service Unavailable.....	140
19821 - Communication Agent Routed Service Degraded.....	140
19822 - Communication Agent Routed Service Congested.....	141
19823 - Communication Agent Routed Service Using Low-Priority Connection Group.....	141
19824 - Communication Agent Pending Transaction Utilization.....	142
19825 - Communication Agent Transaction Failure Rate.....	142
19826 - Communication Agent Connection Congested.....	143
19830 - Communication Agent Service Registration State Change.....	144
19831 - Communication Agent Service Operational State Changed.....	144
19832 - Communication Agent Reliable Transaction Failed.....	145
19833 - Communication Agent Service Egress Message Discarded.....	145
19842 - Communication Agent Resource-Provider Registered.....	146
19843 - Communication Agent Resource-Provider Resource State Changed.....	146
19844 - Communication Agent Resource-Provider Stale Status Received.....	146
19845 - Communication Agent Resource-Provider Deregistered.....	147
19846 - Communication Agent Resource Degraded.....	147
19847 - Communication Agent Resource Unavailable.....	147
19848 - Communication Agent Resource Error.....	148
19850 - Communication Agent Resource-User Registered.....	149
19851 - Communication Agent Resource-User Deregistered.....	149
19852 - Communication Agent Resource Routing State Changed.....	149
19853 - Communication Agent Resource Egress Message Discarded.....	149
19854 - Communication Agent Resource-Provider Tracking Table Audit Results.....	150
19855 - Communication Agent Resource Has Multiple Actives.....	150
19856 - Communication Agent Service Provider Registration State Changed.....	151
19857 - Communication Agent Service Provider Operational State Changed.....	151
19858 - Communication Agent Connection Rejected.....	152
19860 - Communication Agent Configuration Daemon Table Monitoring Failure.....	152
19861 - Communication Agent Configuration Daemon Script Failure.....	153
19862 - Communication Agent Ingress Stack Event Rate.....	153
19863 - Communication Agent Max Connections Limit In Connection Group Reached.....	154
19864 - ComAgent Successfully Set Host Server Hardware Profile.....	154
19865 - ComAgent Failed to Set Host Server Hardware Profile.....	155
19866 - Communication Agent Peer Group Status Changed.....	155

19867 - Communication Agent Peer Group Egress Message Discarded.....	155
19868 - Communication Agent Connection Rejected - Incompatible Network.....	156
EXG Stack (19000-19999).....	156
19900 - DP Server CPU utilization.....	156
19901 - CFG-DB Validation Error.....	157
19902 - CFG-DB Update Failure.....	157
19903 - CFG-DB post-update Error.....	158
19904 - CFG-DB post-update Failure.....	158
19905 - Measurement Initialization Failure.....	159
19910 - Message Discarded at Test Connection.....	159
19911 - Test message discarded	160
Platform (31000-32800).....	160
31000 - S/W fault.....	160
31001 - S/W status.....	160
31002 - Process watchdog failure.....	161
31003 - Tab thread watchdog failure.....	161
31100 - Database replication fault.....	162
31101 - Database replication to slave failure.....	162
31102 - Database replication from master failure.....	162
31103 - DB Replication update fault.....	163
31104 - DB Replication latency over threshold.....	163
31105 - Database merge fault.....	164
31106 - Database merge to parent failure.....	164
31107 - Database merge from child failure.....	164
31108 - Database merge latency over threshold.....	165
31109 - Topology config error.....	165
31110 - Database audit fault.....	166
31111 - Database merge audit in progress.....	166
31112 - DB replication update log transfer timed out.....	166
31113 - DB replication manually disabled.....	167
31114 - DB replication over SOAP has failed.....	167
31115 - Database service fault.....	168
31116 - Excessive shared memory.....	168
31117 - Low disk free.....	168
31118 - Database disk store fault.....	169
31119 - Database updatelog overrun.....	169
31120 - Database updatelog write fault.....	170
31121 - Low disk free early warning.....	170
31122 - Excessive shared memory early warning.....	170
31123 - Database replication audit command complete.....	171
31124 - ADIC error.....	171

31125 - Database durability degraded.....	172
31126 - Audit blocked.....	172
31127 - DB Replication Audit Complete.....	172
31128 - ADIC Found Error.....	173
31129 - ADIC Found Minor Issue.....	173
31130 - Network health warning.....	173
31131 - DB Ousted Throttle Behind.....	174
31140 - Database perl fault.....	174
31145 - Database SQL fault.....	175
31146 - DB mastership fault.....	175
31147 - DB upsynclog overrun.....	175
31148 - DB lock error detected.....	176
31200 - Process management fault.....	176
31201 - Process not running.....	177
31202 - Unkillable zombie process.....	177
31206 - Process mgmt monitoring fault.....	178
31207 - Process resource monitoring fault.....	178
31208 - IP port server fault.....	178
31209 - Hostname lookup failed.....	179
31213 - Process scheduler fault.....	179
31214 - Scheduled process fault.....	180
31215 - Process resources exceeded.....	180
31216 - SysMetric configuration error.....	180
31220 - HA configuration monitor fault.....	181
31221 - HA alarm monitor fault.....	181
31222 - HA not configured.....	182
31223 - HA Heartbeat transmit failure.....	182
31224 - HA configuration error.....	182
31225 - HA service start failure.....	183
31226 - HA availability status degraded.....	183
31227 - HA availability status failed.....	183
31228 - HA standby offline.....	184
31229 - HA score changed.....	184
31230 - Recent alarm processing fault.....	185
31231 - Platform alarm agent fault.....	185
31232 - Late heartbeat warning.....	185
31233 - HA Path Down.....	186
31234 - Untrusted Time Upon Initialization	186
31235 - Untrusted Time After Initialization	187
31236 - HA Link Down.....	187
31240 - Measurements collection fault.....	188

31250 - RE port mapping fault.....	188
31260 - SNMP Agent.....	188
31270 - Logging output.....	189
31280 - HA Active to Standby transition.....	189
31281 - HA Standby to Active transition.....	189
31282 - HA Management Fault.....	190
31283 - Lost Communication with server.....	190
31284 - HA Remote Subscriber Heartbeat Warning.....	191
31285 - HA Node Join Recovery Entry.....	191
31286 - HA Node Join Recovery Plan.....	191
31287 - HA Node Join Recovery Complete.....	192
31290 - HA Process Status.....	192
31291 - HA Election Status.....	193
31292 - HA Policy Status.....	193
31293 - HA Resource Link Status.....	193
31294 - HA Resource Status.....	194
31295 - HA Action Status.....	194
31296 - HA Monitor Status.....	194
31297 - HA Resource Agent Info.....	195
31298 - HA Resource Agent Detail.....	195
31299 - HA Notification Status.....	195
31300 - HA Control Status.....	196
31301 - HA Topology Events.....	196
32100 - Breaker Panel Feed Unavailable.....	196
32101 - Breaker Panel Breaker Failure.....	197
32102 - Breaker Panel Monitoring Failure.....	197
32103 - Power Feed Unavailable.....	197
32104 - Power Supply 1 Failure.....	198
32105 - Power Supply 2 Failure.....	198
32106 - Power Supply 3 Failure.....	198
32107 - Raid Feed Unavailable.....	199
32108 - Raid Power 1 Failure.....	199
32109 - Raid Power 2 Failure.....	199
32110 - Raid Power 3 Failure.....	200
32111 - Device Failure.....	200
32112 - Device Interface Failure.....	200
32113 - Uncorrectable ECC memory error.....	201
32114 - SNMP get failure.....	201
32115 - TPD NTP Daemon Not Synchronized Failure.....	202
32116 - TPD Server's Time Has Gone Backwards.....	202
32117 - TPD NTP Offset Check Failure.....	203

32300 - Server fan failure.....	204
32301 - Server internal disk error.....	204
32302 - Server RAID disk error.....	205
32303 - Server Platform error.....	205
32304 - Server file system error.....	206
32305 - Server Platform process error.....	206
32306 - Server RAM shortage error.....	207
32307 - Server swap space shortage failure.....	207
32308 - Server provisioning network error.....	207
32309 - Eagle Network A Error.....	208
32310 - Eagle Network B Error.....	208
32311 - Sync Network Error.....	209
32312 - Server disk space shortage error.....	209
32313 - Server default route network error.....	210
32314 - Server temperature error.....	211
32315 - Server mainboard voltage error.....	212
32316 - Server power feed error.....	212
32317 - Server disk health test error.....	213
32318 - Server disk unavailable error.....	213
32319 - Device error.....	214
32320 - Device interface error.....	214
32321 - Correctable ECC memory error.....	215
32322 - Power Supply A error.....	215
32323 - Power Supply B error.....	216
32324 - Breaker panel feed error.....	216
32325 - Breaker panel breaker error.....	217
32326 - Breaker panel monitoring error.....	220
32327 - Server HA Keepalive error.....	221
32328 - DRBD is unavailable.....	221
32329 - DRBD is not replicating.....	222
32330 - DRBD peer problem.....	222
32331 - HP disk problem.....	222
32332 - HP Smart Array controller problem.....	223
32333 - HP hpacucliStatus utility problem.....	223
32334 - Multipath device access link problem.....	224
32335 - Switch link down error.....	225
32336 - Half Open Socket Limit.....	225
32337 - E5-APP-B Firmware Flash.....	226
32338 - E5-APP-B Serial mezzanine seating.....	226
32339 - TPD Max Number Of Running Processes Error.....	226
32340 - TPD NTP Daemon Not Synchronized Error.....	227

32341 - TPD NTP Daemon Not Synchronized Error.....	228
32342 - NTP Offset Check Error.....	228
32343 - TPD RAID disk	229
32344 - TPD RAID controller problem.....	230
32345 - Server Upgrade snapshot(s) invalid.....	230
32346 - OEM hardware management service reports an error.....	231
32347 - The hwmgmtcliStatus daemon needs intervention.....	231
32348 - The FIPS subsystem needs intervention.....	232
32349 - HIDS has detected file tampering.....	232
32350 - Security Process Terminated.....	232
32500 - Server disk space shortage warning.....	233
32501 - Server application process error.....	233
32502 - Server hardware configuration error.....	234
32503 - Server RAM shortage warning.....	234
32504 - Software Configuration Error.....	235
32505 - Server swap space shortage warning.....	235
32506 - Server default router not defined.....	236
32507 - Server temperature warning.....	237
32508 - Server core file detected.....	237
32509 - Server NTP Daemon not synchronized.....	238
32510 - CMOS battery voltage low.....	239
32511 - Server disk self test warning.....	239
32512 - Device warning.....	240
32513 - Device interface warning.....	240
32514 - Server reboot watchdog initiated.....	241
32515 - Server HA failover inhibited.....	241
32516 - Server HA Active to Standby transition.....	241
32517 - Server HA Standby to Active transition.....	242
32518 - Platform Health Check failure.....	242
32519 - NTP Offset Check failure.....	243
32520 - NTP Stratum Check failure.....	243
32521 - SAS Presence Sensor Missing.....	244
32522 - SAS Drive Missing.....	245
32523 - DRBD failover busy.....	245
32524 - HP disk resync.....	245
32525 - Telco Fan Warning.....	246
32526 - Telco Temperature Warning.....	247
32527 - Telco Power Supply Warning.....	247
32528 - Invalid BIOS value.....	247
32529 - Server Kernel Dump File Detected.....	248
32530 - TPD Upgrade Failed.....	248

32531 - Half Open Socket Warning Limit.....	249
32532 - Server Upgrade Pending Accept/Reject.....	249
32533 - TPD Max Number Of Running Processes Warning.....	250
32534 - TPD NTP Source Is Bad Warning.....	250
32535 - TPD RAID disk resync.....	251
32536 - TPD Server Upgrade snapshot(s) warning.....	251
32537 - FIPS subsystem warning event.....	252
32700 - Telco Switch Notification.....	252
32701 - HIDS Initialized.....	252
32702 - HIDS Baseline Deleted.....	253
32703 - HIDS Enabled.....	253
32704 - HIDS Disabled.....	253
32705 - HIDS Monitoring Suspended.....	254
32706 - HIDS Monitoring Resumed.....	254
32707 - HIDS Baseline Updated.....	254

Chapter 4: Key Performance Indicators (KPIs).....256

General KPIs information.....	257
KPIs overview.....	257
KPIs.....	257
Viewing KPIs.....	257
KPIs data export elements.....	257
Exporting KPIs.....	258
EXHR KPIs.....	259
PDBI KPIs.....	260
SS7/Sigtran KPIs.....	261
Throttling KPIs.....	261

Chapter 5: Measurements.....263

General measurements information.....	264
Measurements.....	264
Measurement elements.....	264
Generating a measurements report.....	265
Measurements data export elements.....	266
Exporting measurements reports.....	267
Communication Agent (ComAgent) Exception measurements.....	268
CADataFIFOQueueFul.....	272
CADSTxDscrdCong	272
CAHSRsrcErr.....	273
CAHSTxDscrdCongSR.....	273

CAHSTxDscrdIntErrSR.....	274
CAHSTxDscrdUnavailSR.....	274
CAHSTxDscrdUnknownSR.....	275
CAHSTxDscrdUnkwnRsrc.....	276
CAHSTxRsrc.....	276
CAMxFIFOQueueFul.....	276
CAPSTxDscrdUnkwnGrp.....	277
CAPSTxDscrdUnavailGrp.....	277
CAPSTxDscrdCongPeer.....	278
CARsrcPoolFul	278
CARSTxDscrdCong	279
CARSTxDscrdInternalErr.....	280
CARSTxDscrdSvcUnavail	280
CARxDiscUnexpEvent	281
CARxDscrdBundle.....	281
CARxDscrdConnUnavail.....	281
CARxDscrdDecodeFailed	282
CARxDscrdIncompat	282
CARxDscrdInternalErr	283
CARxDscrdLayerSendFail	283
CARxDscrdMsgLenErr	284
CARxDscrdUnkServer	284
CARxDscrdUnkStkLyr	285
CARxMsgUnknown	285
CAStackQueueFul	285
CATransDscrdInvCorrId	286
CATransDscrdStaleErrRsp	286
CATransEndAbnorm	287
CATransEndAbnormRateAvg	287
CATransEndAbnormRateMax	288
CATransEndAnsErr	288
CATransEndErr	289
CATransEndNoResources.....	289
CATransEndNoResponse.....	290
CATransEndUnkwnSvc.....	290
CATransEndUnregSvc	291
CATransNoReTxMaxTTL.....	291
CATransRetx	292
CATransReTxExceeded.....	292
CATransStaleSuccessRsp	293
CATransTTLExceeded.....	294

CATxDscrdBundle.....	294
CATxDscrdConnUnAvail.....	295
CATxDscrdDestUserIncmpat.....	295
CATxDscrdEncodeFail.....	295
CATxDscrdInternalErr	296
CATxDscrdMxSendFail.....	296
CATxDscrdUnknownSvc	297
CATxDscrdUnkServer	297
CATxDscrdUnregSvc	298
Communication Agent (ComAgent) Performance measurements.....	298
CAAvgDataFIFOQueueUtil.....	300
CAAvgMxFIFOQueueUtil.....	301
CAAvgQueueUtil	302
CAAvgRsrcPoolUtil	302
CAAvgRxStackEvents	303
CAAvgTxStackEvents	303
CADSTx	303
CAHSTxRsrc.....	304
CAHSTxRsrcRateAvg.....	304
CAHSTxRsrcRateMax.....	305
CAPeakDataFIFOQueueUtil.....	305
CAPeakMxFIFOQueueUtil.....	305
CAPeakQueueUtil	306
CAPeakRsrcPoolUtil	306
CAPeakRxStackEvents	307
CAPeakTxStackEvents	307
CAPSTxGrp.....	308
CAPSTxGrpSuccess.....	308
CARSTx	309
CARx.....	309
CARxBundled.....	309
CARxEventsBundled.....	310
CARxSuccess.....	310
CATransEndAbnorm	311
CATransEndAbnormRateAvg	311
CATransEndAbnormRateMax	312
CATransEndNorm.....	312
CATransPendingAvg	313
CATransPendingMax	313
CATransRateAvg	313
CATransRateMax	314

CATransStarted	314
CATransTimeAvg	315
CATransTimeMax	315
CATx.....	315
CATxBundled.....	316
CATxEventsBundled.....	316
CATxSuccess.....	317
HLR Measurements.....	317
EXHR measurements.....	317
EXHRTT measurements.....	318
PDBI measurements.....	319
PDE measurements.....	321
OAM measurements.....	322
OAM.ALARM measurements.....	322
OAM.SYSTEM measurements.....	322
SS7/Sigtran Measurements.....	324
SS7/Sigtran measurements overview.....	324
Association Exception measurements.....	324
Association Performance measurements.....	334
Association Usage measurements.....	336
Link Exception measurements.....	338
Link Performance measurements.....	341
Link Set Performance measurements.....	344
Link Set Usage measurements.....	346
Link Usage measurements.....	347
Server M3UA Exception measurements.....	350
Server M3UA Performance measurements.....	354
Server M3UA Usage measurements.....	360
Server MTP3 Exception measurements.....	364
Server MTP3 Performance measurements.....	369
Server Resource Usage measurements.....	373
Server SCCP Exception measurements.....	379
Server SCCP Performance measurements.....	395
Throttling measurements.....	404
ThrottleAllow.....	405
ThrottleDiscard.....	406
ThrottleDiscardByName.....	406
ThrottleDiscardTCAP.....	406
ThrottleDiscardUDTS.....	407
ThrottleMatch.....	407
ThrottleMatchByName.....	407

ThrottleSimulation.....	408
ThrottleWhitelistHit.....	408
ThrottleWhitelistMiss.....	409
Transport Exception measurements.....	409
RxTrFarEndClose.....	410
EvTrManClose.....	411
EvTrNoRespClose.....	411
EvTrCnxFail.....	412
TxTrSendFail.....	413
RxTrRecvFailed.....	413
EvTrSockInitFail.....	414
TmSingleTransQueueFull.....	414
EvSctpAdjPToDwn.....	415
EvSctpTransRej.....	416
Transport Usage measurements.....	417
EvTrCnxSuccess.....	417
TmTrEnaNotUp.....	418
RxTmSctpBufAvg.....	419
RxTmSctpBufPeak.....	419
Transport Performance measurements.....	420
TxTrOctets.....	421
RxTrOctets.....	421
TmSingleTransQueuePeak.....	422
TmSingleTransQueueAvg.....	423
SctpTransPeerCWNDPeak.....	423
SctpTransPeerCWNDAvg.....	424
SctpTransPeerSRTTPeak.....	424
SctpTransPeerSRTTAvg.....	424
SctpTransUnAckedDataPeak.....	425
SctpTransUnAckedDataAvg.....	425
SctpTransRTOPeak.....	426
SctpTransRTOAvg.....	426
Glossary.....	428

List of Figures

Figure 1: Flow of Alarms.....39

Figure 2: Alarm Indicators Legend.....40

Figure 3: Trap Count Indicator Legend.....40

Figure 4: Breaker Panel LEDs.....218

Figure 5: Breaker Panel Setting.....219

List of Tables

Table 1: Admonishments.....25

Table 2: Data Export Elements.....30

Table 3: Active Tasks Elements.....33

Table 4: Active Tasks Report Elements.....35

Table 5: Scheduled Tasks Elements.....36

Table 6: Alarm/Event ID Ranges.....41

Table 7: Alarm and Event Types.....41

Table 8: Schedule Active Alarm Data Export Elements.....43

Table 9: Schedule Event Data Export Elements.....46

Table 10: Security Log View History Elements.....49

Table 11: Schedule Security Log Data Export Elements.....50

Table 12: Schedule KPI Data Export Elements.....258

Table 13: EXHR KPIs.....259

Table 14: PDBI KPIs.....260

Table 15: SS7/Sigtran KPIs.....261

Table 16: Throttling KPIs.....261

Table 17: Measurements Elements.....265

Table 18: Schedule Measurement Data Export Elements.....266

Table 19: Communication Agent Exception Measurement Report Fields.....268

Table 20: Communication Agent Performance Measurement Report Fields.....298

Table 21: EXHR Measurement Report Fields.....317

Table 22: EXHRTT Measurement Report Fields.....318

Table 23: PDBI Measurement Report Fields.....	319
Table 24: PDE Measurement Report fields.....	321
Table 25: OAM Alarm Measurements.....	322
Table 26: OAM System Measurements.....	322
Table 27: Association Exception Measurement Report Fields.....	324
Table 28: Association Performance Measurement Report Fields.....	334
Table 29: Association Usage Measurement Report Fields.....	336
Table 30: Link Exception Measurement Report Fields.....	338
Table 31: Link Performance Measurement Report Fields.....	341
Table 32: Link Set Performance Measurement Report Fields.....	344
Table 33: Link Set Usage Measurement Report Fields.....	346
Table 34: Link Usage Measurement Report Fields.....	347
Table 35: Server M3UA Exception Measurement Report Fields.....	350
Table 36: Server M3UA Performance Measurement Report Fields.....	354
Table 37: Server M3UA Usage Measurement Report Fields.....	360
Table 38: Server MTP3 Exception Measurement Report Fields.....	364
Table 39: Server MTP3 Performance Measurement Report Fields.....	369
Table 40: Server Resource Usage Measurement Report Fields.....	373
Table 41: Server SCCP Exception Measurement Report Fields.....	379
Table 42: Server SCCP Performance Measurement Report Fields.....	395
Table 43: Throttling Measurements.....	404

Chapter 1

Introduction

Topics:

- *Overview.....24*
- *Scope and Audience.....24*
- *Manuel Organization.....24*
- *Documentation Admonishments.....25*
- *Related Publications.....25*
- *Locate Product Documentation on the Oracle Help Center Site.....26*
- *Customer Training.....26*
- *My Oracle Support (MOS).....27*
- *Emergency Response.....27*

This chapter contains an overview of the available information for HLR 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 *HLR Alarms, KPIs, and Measurements* documentation provides information about HLR 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 HLR. The manual provides lists of alarms, events, KPIs, and measurements along with preventive and corrective procedures that will aid personnel in maintaining the HLR.

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.

Manuel Organization





Information in this document is organized into chapters:

- *Introduction* contains general information about the scope and audience of this manual, the organization of this document, and how to get technical assistance.
- *Alarms and Events, KPIs, and Measurements Overview* contains an overview of alarms, events, KPIs, and measurements information.
- *Alarms and Events* contains detailed information and recovery procedures for alarms and events.
- *Key Performance Indicators (KPIs)* contains detailed KPI information
- *Measurements* contains detailed measurement information and recovery procedures

Documentation Admonishments

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

Table 1: Admonishments

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

Related Publications

The HLR Router documentation set includes these publications, which provide information for the configuration and use of HLR Router and related applications.

Some documents are available only through the Oracle Technical Network (OTN).

The current releases of all documents are available through the Oracle Technical Network

Getting Started includes a product overview, system architecture, and functions. It also explains the HLR Router GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the HLR Router, both for initial setup and maintenance.

HLR Router Online Help explains how to use the HLR Router GUI pages to manage the configuration and maintenance of the EAGLE XG Database and the Tekelec HLR Router.

HLR Router Administration Guide describes HLR Router architecture, functions, system and PDBI configuration; Signaling and Transport configuration; the Query Server; and PDE CSV file formats.

HLR Router Alarms, KPIs, and Measurements Reference Guide provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

SS7/Sigtran User Guide describes HLR Router's Signaling Network Interface, which provides standard SCCP functionality, traditional MTP3 routing capabilities, and a standard M3UA interface to the external network. The SS7/Sigtran section of the documentation explains how to use the SS7/Sigtran GUI pages to perform configuration and maintenance tasks related to adjacent servers, SS7 signaling points, link sets, associations, routes, and SS7/Sigtran options.

Transport Manager User Guide describes the configuration of Transports (SCTP associations and UDP connections with remote hosts over an underlying IP network).

Locate Product Documentation on the Oracle Help Center Site

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

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

Customer Training

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

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

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

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

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

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

Chapter 2

Alarms and Events, KPIs, and Measurements Overview

Topics:

- *Displaying the file list.....29*
- *Opening a file.....29*
- *Data Export.....29*
- *Tasks.....32*

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

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

Opening a file

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

1. Select **Status & Manage > Files**.
2. Select an **NE Name**.
3. Click **List Files**.

The **Status & Manage Files** list page for the selected network element displays all files stored in its file management storage area.

4. Click the **Filename** of the file to be opened.
5. Click **Open** to open the file.

Data Export

From the Data Export page you can set an export target to receive exported selected data. Several types of 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 **Administration > Remote Servers > Data Export** page.

Table 2: Data Export Elements

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

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

Configuring data export

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

1. Select **Administration > Remote Servers > Data Export**.
2. Enter a **Hostname**.
See [Data Export elements](#) for details about the **Hostname** field and other fields that appear on this page.

3. Enter a **Username**.
4. Enter a **Directory Path** on the Export server.
5. 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.
13. Enter the password.
The server attempts to exchange keys with the export server currently defined on the page. After the SSH keys are successfully exchanged, continue with the next step.
14. Click **OK** to apply the changes or **Cancel** to discard the changes.
The export server is now configured and available to receive performance and configuration data.
15. You may optionally click **Test Transfer** to confirm the ability to export to the server currently defined on the page.
The user can monitor the progress of the task by selecting the **Tasks** drop down list in the page control area.

Tasks

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

Active Tasks

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

Active Tasks elements

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

Table 3: Active Tasks Elements

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

Deleting a task

Use this procedure to delete one or more tasks.

1. Select **Status & Manage > Tasks > Active Tasks**.
2. Select a server.

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

All active tasks on the selected server are displayed.

3. Select one or more tasks.

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

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

4. Click **Delete**.
5. Click **OK** to delete the selected task(s).
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**.
2. Select a server.

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

All active tasks on the selected server are displayed.

3. Click **Delete all Completed**.

4. Click **OK** to delete all completed tasks.
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**.
2. Select a server.

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

All active tasks on the selected server are displayed.

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

Pausing a task

Use this procedure to pause a task.

1. Select **Status & Manage > Tasks > Active Tasks**.
2. Select a server.

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

All active tasks on the selected server are displayed.

3. Select a task.

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

4. Click **Pause**.
A confirmation box appears.
5. Click **OK** to pause the selected task.
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**.
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

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

Generating an active task report

Use this procedure to generate an active task report.

1. Select **Status & Manage > Tasks > Active Tasks**.
2. Select a server.

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

All active tasks on the selected server are displayed.

3. Select one or more tasks.

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

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

Scheduled Tasks

The periodic export of certain data can be scheduled through the GUI. The **Scheduled Tasks** page provides you with a location to view, edit, delete, and generate reports of these scheduled tasks. For more information about the types of data that can be exported, see:

- [Exporting active alarms](#)
- [Exporting alarm and event history](#)
- [Exporting KPIs](#)
- [Exporting measurements reports](#)

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

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

Editing a scheduled task

Use this procedure to edit a scheduled task.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.
All scheduled tasks are displayed on the **Scheduled Tasks** page.
2. Select a task.
3. Click **Edit**.
The **Data Export** page for the selected task appears.
4. Edit the available fields as necessary.
See [Scheduled Tasks elements](#) for details about the fields that appear on this page.
5. Click **OK** or **Apply** to submit the changes and return to the **Scheduled Tasks** page.

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

1. Select **Status & Manage > Tasks > Scheduled Tasks**.
All scheduled tasks are displayed on the **Scheduled Tasks** page.
2. Select one or more tasks.
3. Click **Delete**.
4. Click **OK** to delete the selected task(s).
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**.
All scheduled tasks are displayed on the **Scheduled Tasks** page.
2. Select one or more tasks.
Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.
3. Click **Report**.
4. Click **Print** to print the report.
5. Click **Save** to save the report.

Chapter 3

Alarms and Events

Topics:

- [General alarms and events information.....39](#)
- [OAM \(10000-10999\).....52](#)
- [HLR Alarms \(14000-14999\).....73](#)
- [SS7/Sigtran Alarms \(19200-19299\).....90](#)
- [Transport Manager Alarms and Events \(19400-19499\).....121](#)
- [Communication Agent, ComAgent \(19800-19909\).....129](#)
- [EXG Stack \(19000-19999\).....156](#)
- [Platform \(31000-32800\).....160](#)

This section provides general alarm/event information, and lists the types of alarms and events that can occur on the system. Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the **Alarms & Events > View Active** GUI menu option. The alarms and events log can be viewed from the **View History** GUI menu option.

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

General alarms and events information

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

Alarms and events overview

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

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

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

Events note the occurrence of a transient condition. Events have a severity of Info and are logged on the **View History** page.

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

Figure 1: Flow of Alarms shows how Alarms and Events are organized in the application.

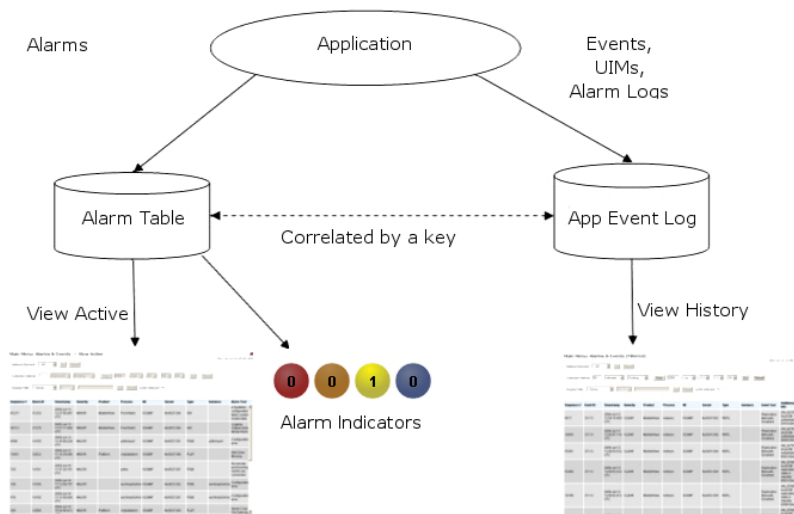


Figure 1: Flow of Alarms

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

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

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








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

Figure 2: Alarm Indicators Legend



	Trap count > 0 (bright blue)
	Trap count = 0 (pale blue)

Figure 3: Trap Count Indicator Legend

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

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

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

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

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

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

Alarm and event ID ranges

The AlarmID listed for each alarm has a process classification:

Table 6: Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
OAM	10000-10999
HLR Router	14000-14999
SS7/SIGTRAN	19200-19299
Transport Manager	19400-19499
EXG Stack	19000-19999
Platform	31000-32700

Alarm and event types

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

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

Table 7: Alarm and Event Types

Type Name	Type
APPL	Application
CAF	Communication Agent (ComAgent)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
CHG	Charging
CNG	Congestion Control
COLL	Collection
DAS	Diameter Application Server (Message Copy)

Type Name	Type
DB	Database
DIAM	Diameter
DISK	Disk
DNS	Domain Name Service
DPS	Data Processor Server
ERA	Event Responder Application
FABR	Full Address Based Resolution
HA	High Availability
HTTP	Hypertext Transfer Protocol
IDIH	Integrated DIH
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOADGEN	Load Generator
LOG	Logging
MEAS	Measurements
MEM	Memory
NAT	Network Address Translation
NP	Number Portability
OAM	Operations, Administration & Maintenance
PCRF	Policy Charging Rules Function
PDRA	Policy Diameter Routing Agent
PLAT	Platform
PROC	Process
PROV	Provisioning
pSBR	Policy SBR
QP	QBus
RBAR	Range-Based Address Resolution
REPL	Replication
SCTP	Stream Control Transmission Protocol
SDS	Subscriber Database Server

Type Name	Type
SIGC	Signaling Compression
SIP	Session Initiation Protocol Interface
SL	Selective Logging
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack
SW	Software (generic event type)
TCP	Transmission Control Protocol

Viewing active alarms

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

Use this procedure to view active alarms.

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

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

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

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox

Element	Description	Data Input Notes
		Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting 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 and 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. For more information about fields on this page, see [Active alarms data export elements](#).
4. Enter the **Task Name**.
5. Select the **Export Frequency**.
6. Select the **Time of Day**.
Note: **Time of Day** is not an option if **Export Frequency** equals **Once**.
7. Select the **Day of Week**.
Note: **Day of Week** is not an option if **Export Frequency** equals **Once**.
8. Click **OK** or **Apply** to initiate the active alarms export task.
From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see [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_180627.csv.

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

Generating a report of active alarms

Use this procedure to generate a report.

1. Select **Alarms & Events > View Active**.
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 NOAM or SOAM. Alarm collection is handled solely by NOAM 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

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

Element	Description	Data Input Notes
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: 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

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 is 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, and schedule a data export task.

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

The **View History** page appears.

2. If necessary, specify filter criteria and click **Go**.
The historical alarms and events are displayed according to the specified criteria.
3. Click **Export**.
The **Schedule Event Data Export** page appears.
4. Enter the **Task Name**.
For more information about **Task Name**, or any field on this page, see [Historical events data export elements](#).
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes**.
7. Select the **Time of Day**.

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

8. Select the **Day of Week**.
Note: **Day of Week** is not an option if **Export Frequency** equals **Once**.
9. Click **OK** or **Apply** to initiate the data export task.
The data export task is scheduled. From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see [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.

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.

Security Log View History elements

This table describes the elements of the **Security Log > View History** page.

Table 10: Security Log View History Elements

Security Log History Element	Element Description
Timestamp	The date and time the security record was generated (fractional seconds resolution).
User	The user initiating the action.
Sess ID	The session identifier.
Remote IP	The remote IP address for the user.
Message	Summary details about the action which generated the security record.
Status	The status of the action, either SUCCESS or ERROR .
Screen	The page on which the action occurred, the Login page, for example.
Action	The user action, login, for example.
Details	Additional details about the action which generated the security record.
Server	The server which processed the action.

Viewing security log files

Use this procedure to view security log files.

1. Select **Security Log > View History**.
The **View History** page appears.
2. Specify the **Collection Interval**.
3. If necessary, specify filter criteria and click **Go**.

Note: Some fields, such as **Details**, 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.

The security log history displays sorted by collection time stamp.

Note: There are two relevant time stamps for the security log: the time stamp of the event and the time stamp for when the record was merged. The time stamps display initially using the source time, which makes the report appear unordered. However, the report is indeed sorted by collection time.

Security log data export elements

This table describes the elements on the **Security Log > View History [Export]** page.

Table 11: Schedule Security Log Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Once, Hourly, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Export Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Textbox or Scrolling List Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Scrolling List Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting security log files

You can schedule periodic exports of security log data from the **Security Log View History** page. Security log 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](#).

Use this procedure to export security log files and to schedule a data export task.

1. Select **Security Log > View History**.

The **View History** page appears.

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

The security log files are displayed according to the specified criteria.

3. Click **Export**.

The **Schedule Security Log Data Export** page appears.

4. Enter the **Task Name**.

For more information about **Task Name**, or any field on this page, see [Security log data export elements](#).

5. Enter a **Description** for the export task.

6. Select the **Export Frequency**.

7. If you selected Hourly as the export frequency, select the **Minute** of each hour for the data export.

8. Select the **Time of Day**.

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

9. Select the **Day of Week**.

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

10. Click **OK** or **Apply** to initiate the security log 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](#)

11. Click **Export**.

The file is exported.

12. 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 security log history you exported during this procedure.

If an export fails for any reason, an error message appears indicating this failure.

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

Generating a Security Log report

Use this procedure to generate a report.

1. Select **Security Log > View History**.
The **View History** page appears.
2. Specify the **Collection Interval**.
3. Specify the filter criteria, if necessary, and click **Go**.
The security log files 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.
4. Click **Report**.
The Security Log Report is generated. This report can be printed or saved to a file.
5. Click **Print** to print the report.
6. Click **Save** to save the report to a file.

OAM (10000-10999)

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

10000 - Incompatible database version

Alarm Group:	DB
Description:	The database version is incompatible with the installed software database version.
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 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: 1
OID: tekelecRestoreCompleteNotify
Recovery:
 No action required.

10006 - Database restoration failed

Event Type: DB
Description: The database restoration has failed.
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 1
OID: tekelecRestoreFailNotify
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

10008 - Database provisioning manually disabled

Alarm Group: DB
Description: Database provisioning has been manually disabled.
Severity: Minor
Instance: N/A
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecProvisioningManuallyDisabledNotify

Recovery:
No action required.

10009 - Config and Prov db not yet synchronized

Alarm Group: REPL
Description: The configuration and the provisioning databases are not yet synchronized.
Severity: Critical
Instance: N/A
HA Score: Failed
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7OAGTCfgProvDbNoSyncNotify

Recovery:

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

10010 - Stateful db from mate not yet synchronized

Alarm Group: HA
Description: The stateful database is not synchronized with the mate database.
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 Group: OAM
Description: Monitoring for table cannot be set up.
Severity: Major
Instance: N/A

HA Score: Degraded
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7OAGTCantMonitorTableNotify
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

10012 - Table change responder failed

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

10013 - Application restart in progress

Alarm Group: HA
Description: An application restart is in progress.
Severity: Minor
Instance: N/A
HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: awpss7OAGTAppISWDisabledNotify
Recovery:
 If duration of alarm is greater than two seconds, contact [My Oracle Support \(MOS\)](#).

10020 - Backup failure

Alarm Group: DB
Description: Database backup failed.
Severity: Minor
Instance: N/A

HA Score: Normal
Auto Clear Seconds: This alarm does not autoclear.
OID: 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 Group: AUD
Description: Database backup failed.
Severity: Minor
Instance:
HA Score: Normal
Auto Clear Seconds: 0
OID: awpss7TekelecResourceAuditFailureNotify

Recovery:**10051 - Route Deployment Failed**

Alarm Group: 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 Group: AUD
Description: An error occurred in the discovery of network routes.
Severity: Minor
Instance: N/A
HA Score: Normal

Auto Clear Seconds: 0
OID: awpss7TekelecRouteDiscoveryFailedNotify

Recovery:

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

10053 - Route deployment failed - no available device

Alarm Group: AUD
Description: A suitable device could not be identified for the deployment of a network route.
Severity: Minor
Instance: Route ID that failed to deploy
HA Score: Normal
Auto Clear Seconds: 0
OID: awpss7TekelecNoRouteDeviceNotify

Recovery:

1. 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 Group: AUD
Description: An error occurred in the deployment of a network device.
Severity: Minor
Instance: Device name that failed to deploy
HA Score: Normal
Auto Clear Seconds: 0
OID: awpss7TekelecDeviceDeploymentFailedNotify

Recovery:

Edit or delete the device.

10055 - Device discovery failed

Alarm Group: AUD
Description: An error occurred in the discovery of network devices.
Severity: Minor
Instance: N/A

HA Score:	Normal
Auto Clear Seconds:	0
OID:	awpss7TekelecDeviceDiscoveryFailedNotify

Recovery:

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

10073 - Server Group Max Allowed HA Role Warning

Alarm Group:	HA
Description:	The server group has received the maximum number of allowed HA role warnings.
Severity:	Minor
Instance:	Affected Server Group name
HA Score:	Normal
Auto Clear Seconds:	0
OID:	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 Group:	HA
Description:	The standby server has temporarily degraded while the new active server stabilizes following a switch of activity.
Severity:	Minor
Instance:	N/A
HA Score:	Degraded
Auto Clear Seconds:	This alarm does not autoclear.
OID:	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 Group:	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:	<ol style="list-style-type: none"> 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 Group:	LOG
Description:	A duplicate scheduled log export task has been queued.

Severity:	Minor
Instance:	<Target ID>
	Note: <Target ID> refers to the scheduled task ID found by running a report from Main Menu > Status & Manage > Tasks > Scheduled Tasks .
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7TekelecLogExportDupSchedTaskNotify
Recovery:	
	<ol style="list-style-type: none"> 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 Group:	LOG
Description:	The log export queue is full
Severity:	Minor
Instance:	<Queue Name>
	Note: <Queue Name> refers to the name of the queue used for the export task ID found by running a report from either 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:	
	<ol style="list-style-type: none"> 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.

10110 - Certificate About to Expire

Alarm Group:	AUD
Description:	The certificate expires within 30 days.
Severity:	Minor
Instance:	<CertificateName>
HA Score:	Normal

Auto Clear Seconds: 0 (zero)
OID: certificateAboutToExpire

Recovery:

Contact [My Oracle Support \(MOS\)](#) for assistance.

10111 - Certificate Expired

Alarm Group: AUD
Description: The certificate is expired.
Severity: Major
Instance: <CertificateName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: certificateExpired

Recovery:

Contact [My Oracle Support \(MOS\)](#) for assistance.

10112 - Certificate Cannot Be Used

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

Recovery:

Contact [My Oracle Support \(MOS\)](#) for assistance.

10115 - Health Check Started

Event Type: LOG
Description: Upgrade health check operation started.
Severity: Info
Instance: <>
HA Score: Normal

Throttle Seconds: 0
OID: tekelecLogHealthCheckStart
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

10116 - Health Check Successful

Event Type: LOG
Description: Upgrade health check operation completed successfully.
Severity: Info
Instance: <>
HA Score: Normal
Throttle Seconds: 0
OID: tekelecLogHealthCheckSuccess
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

10117 - Health Check Failed

Event Type: LOG
Description: Upgrade health check operation failed.
Severity: Info
Instance: <>
HA Score: Normal
Throttle Seconds: 0
OID: tekelecLogHealthCheckFailed
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

10118 - Health Check Not Run

Event Type: LOG
Description: Upgrade health check not run.
Severity: Info
Instance: <>
HA Score: Normal

Throttle Seconds: 1
OID: tekelecLogHealthCheckNotRun
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

10120 - Server Group Upgrade Started

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

10121 - Server Group Upgrade Cancelled - Validation Failed

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

10122 - Server Group Upgrade Successful

Event Group: LOG
Description: The server group upgrade operation completed successfully.
Severity: Info
Instance: <ServerGroupName>

HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogSgUpgradeSuccess
Recovery:
No action required.

10123 - Server Group Upgrade Failed

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

10124 - Server Group Upgrade Cancelled - User Request

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

10130 - Server Upgrade Started

Event Group: LOG
Description: The server upgrade operation has started.
Severity: Info
Instance: <HostName>
HA Score: Normal

Throttle Seconds: 1
OID: tekelecLogServerUpgradeStart
Recovery:
 No action required.

10131 - Server Upgrade Cancelled

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

10132 - Server Upgrade Successful

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

10133 - Server Upgrade Failed

Event Group: LOG
Description: The server upgrade operation failed.
Severity: Info
Instance: <HostName>
HA Score: Normal

Throttle Seconds:	1
OID:	tekelecLogServerUpgradeFailed
Recovery:	No action required.

10134 - Server Upgrade Failed

Alarm Group:	LOG
Description:	The server upgrade operation failed.
Severity:	Major
Instance:	<HostName>
HA Score:	Normal
Auto Clear Seconds:	0
OID:	tekelecLogServerUpgradeFailAlm

Recovery:

1. If there are servers in the server group that have successfully upgraded, you will need to individually restart the upgrade on that server. Navigate to the Upgrade page (**Administration > Software Management > Upgrade**).
2. Select the "Server Group" tab containing the server that raised the alarm.
3. Select the individual server(s) and then click the **Server Upgrade** button to start the upgrade on those servers.

Note: Servers cannot be selected across tabs. If there are servers in multiple server groups, you must restart the server upgrade for each additional "Server Group" tab.

4. If no servers in the group have been upgraded, you can select **Auto Upgrade** to upgrade all servers in the server group. If a server upgrade has failed already, the alarm will be cleared when the server begins to upgrade.

Note: The active server in the NO server group will never upgrade automatically.

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

Event Group:	LOG
Description:	SAML Login Successful
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	1
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

Event Group:	LOG
Description:	An attempt to login to the GUI via conventional login or via SSO login failed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecSamlLoginFailed

Recovery:

1. Use correct username and password to log in.
2. For failed SSO login, verify SSO was properly configured. Collect logs and contact [My Oracle Support \(MOS\)](#) if the problem persists.

10200 - Remote database reinitialization in progress

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

Instance:	<hostname of remote server>
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	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 \(MOS\)](#).

HLR Alarms (14000-14999)

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

14100 - PDB interface disabled

Alarm Group:	PDBI
Description:	The PDBI Interface has been manually disabled.
Severity:	Critical
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID	eagleXgHlrRouterPdbiInterfaceDisabledNotify

Recovery

Enable the PDBI interface.

14101 - No remote client connections

Alarm Group:	PDBI
Description:	PDBI is enabled and no remote provisioning clients are connected.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdbiNoRemoteConnectionsNotify

Recovery

1. Log into the primary NOAM.
2. Select **Eagle XG Database > Configuration > PDBI > Connections** and make sure the appropriate PDBI connections are configured. If they are not configured, insert the PDBI connections.
3. Confirm that the remote clients are running.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14102 - PDBI Connection failed

Alarm Group:	PDBI
Description:	Initialization has failed.
Severity:	Major
Instance:	Connection ID : IP Address
HA Score:	Normal
Auto Clear Seconds	300
OID	eagleXgHlrRouterPdbiConnectionFailedNotify

Recovery

1. Check the connectivity between the primary NOAM and the provisioning clients.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14120 - PDBI Connection established

Event Type:	PDBI
Description:	This event is generated each time a remote provisioning client has successfully established a connection.
Severity:	Info
Instance:	Connection ID : IP Address
HA Score:	Normal
Throttle Seconds	5
OID	eagleXgHlrRouterPdbiConnectionEstablishedNotify

Recovery

Informational event; no action required.

14121 - PDBI Connection terminated

Event Type:	PDBI
Description:	This event is generated each time a remote provisioning client connection terminates.
Severity:	Info

Instance:	Connection ID : IP Address
HA Score:	Normal
Throttle Seconds:	5
OID	eagleXgHlrRouterPdbiConnectionTerminatedNotify

Recovery

Informational event; no action required.

14122 - PDBI connection denied

Event Type:	PDBI
Description:	This event is generated each time a local or remote provisioning client initiated connection establishment is denied due to: <ul style="list-style-type: none"> • interface not enabled • connection originating from an unauthorized IP address • maximum number of allowed remote client connections have been reached • connection to standby PDBA not permitted

Severity: Info

Instance: Connection ID : IP Address

HA Score: Normal

Throttle Seconds 5

OID eagleXgHlrRouterPdbiConnectionDeniedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Eagle XG Database > Configuration > PDBI > Connections:**
 - Make sure the Allow Connections box is checked.
 - Check to see if the Maximum Number of Connections on this page has been exceeded.
3. If step 2 does not resolve the alarm, select **Eagle XG Database > Configuration > PDBI > Connections.**
4. Check if the connection listed is an allowed connection.
 - If the connection is not allowed, insert a new connection.
 - If the connection is allowed, click the corresponding **Edit** button and make sure the connection is configured properly.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14140 - PDB import throttled

Alarm Group: PDBI

Description:	PDB import throttled to prevent from overrunning IDB service processes.
Severity:	Minor
Instance:	Connection ID : IP Address
HA Score:	Normal
Auto Clear Seconds	5
OID	eagleXgHlrRouterPdbiImportThrottledNotify

Recovery

1. The alarm is automatically cleared within five seconds of when the throttling subsides.
2. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14150 - PDB import initialization failed

Alarm Group:	PDBI
Description:	Initialization error.
Severity:	Major
Instance:	pdbimport
HA Score:	Normal
Auto Clear Seconds	43200
OID	eagleXgHlrRouterPdbiImportInitializationFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following import options:
 - Remote Import Enabled
 - Remote Import Mode
 - Remote Import Host IP Address
 - Remote Import User
 - Remote Import Password
 - Remote Import Directory
3. Clear any incorrect import options and replace with the correct import configuration.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14151 - PDB import generation failed

Alarm Group:	PDBI
Description:	File import has failed.
Severity:	Major

Instance:	pdbimport
HA Score:	Normal
Auto Clear Seconds	43200
OID	eagleXgHlrRouterPdbiImportGenerationFailedNotify

Recovery

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

14152 - PDB import transfer failed

Alarm Group:	PDBI
Description:	File transfer from remote host has failed.
Severity:	Major
Instance:	pdbimport
HA Score:	Normal
Auto Clear Seconds	43200
OID	eagleXgHlrRouterPdbiImportTransferFailedNotify

Recovery

1. Check the remote host connectivity.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following import options:
 - Remote Import Enabled
 - Remote Import Mode
 - Remote Import Host IP Address
 - Remote Import User
 - Remote Import Password
 - Remote Import Directory
3. Clear any incorrect import options and replace with the correct import configuration.
4. This alarm can be caused by an invalid ssh-key exchange. To recover from an invalid ssh-key that has created in error
 - a) Deselect/clear all the current data fields for remote import, then **Apply** the settings
 - b) Reset all the data fields for remote import, then **Apply** the settings.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14153 - PDB export initialization failed

Alarm Group:	PDBI
Description:	Export initialization error
Severity:	Major

Instance:	pdbexport
HA Score:	Normal
Auto Clear Seconds	43200
OID	eagleXgHlrRouterPdbiExportInitializationFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following export options:
 - Remote Export Transfers Enabled
 - Remote Export Host IP Address
 - Remote Export User
 - Remote Export Password
 - Remote Export Directory
3. Clear any incorrect export options and replace with the correct export configuration.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14154 - PDB export generation failed

Alarm Group:	PDBI
Description:	The scheduled export has failed.
Severity:	Major
Instance:	pdbexport
HA Score:	Normal
Auto Clear Seconds	43200
OID	eagleXgHlrRouterPdbiExportGenerationFailedNotify

Recovery

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

14155 - PDB export transfer failed

Alarm Group:	PDBI
Description:	Failure to transfer file to the remote host
Severity:	Major
Instance:	pdbexport
HA Score:	Normal
Auto Clear Seconds	43200
OID	eagleXgHlrRouterPdbiExportTransferFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Eagle XG Database > Configuration > PDBI > Options** and check the following export options:
 - Remote Export Transfers Enabled
 - Remote Export Host IP Address
 - Remote Export User
 - Remote Export Password
 - Remote Export Directory
3. Clear any incorrect export options and replace with the correct export configuration.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14160 - PDBI Import successful

Event Type:	PDBI
Description:	This event is generated each time a PDBI import is successful.
Severity:	Info
Instance:	pdbiimport
HA Score:	Normal
Throttle Seconds	5
OID	eagleXgHlrRouterPdbiImportOperationCompletedNotify

Recovery

Informational event; no action required.

14161 - PDBI Export successful

Event Type:	PDBI
Description:	This event is generated each time a PDBI export is successful.
Severity:	Info
Instance:	pdbiexport
HA Score:	Normal
Throttle Seconds	5
OID	eagleXgHlrRouterPdbiExportOperationCompletedNotify

Recovery

Informational event; no action required.

14170 - EPAP Audit started and in progress

Event Type:	PDBI
Description:	EPAP Audit started and in progress.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiEpapAuditStartedAndInProgress
Recovery	
No action required.	

14171 - EPAP Audit aborted

Event Type:	PDBI
Description:	EPAP Audit aborted.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiEpapAuditAborted
Recovery	
No action required.	

14172 - EPAP Audit failed to complete

Event Type:	PDBI
Description:	EPAP Audit failed to complete.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiEpapAuditFailedToComplete
Recovery	

This condition may indicate that a connection was down or lost and the audit status shows as **Failed**. It is recommended to contact [My Oracle Support \(MOS\)](#).

14173 - EPAP Audit completed

Event Type:	PDBI
Description:	EPAP Audit completed.
Severity:	Info
Instance:	PDBA
HA Score:	
Throttle Seconds	
OID	pdbiEpapAuditCompleted
Recovery	
	No action required.

14174 - NPA Split activation failed

Event Type:	PDBI
Description:	NPA Split activation failed.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiNpaSplitActivationFailed
Recovery	
	This condition may indicate the system error, and the NPA split status now shows as Failed . It is recommended to contact My Oracle Support (MOS) .

14175 - NPA Split started and is active

Event Type:	PDBI
Description:	NPA Split started and is active.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiNpaSplitStartedAndIsActive
Recovery	
	No action required.

14176 - NPA Split completion failed

Event Type:	PDBI
Description:	NPA Split completion failed.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiNpaSplitCompletionFailed

Recovery

This condition may indicate the system error, and the NPA split status now shows as **Failed**. It is recommended to contact [My Oracle Support \(MOS\)](#).

14177 - NPA Split completed

Event Type:	PDBI
Description:	NPA Split completed.
Severity:	Info
Instance:	PDBA
HA Score:	Normal
Throttle Seconds	30
OID	pdbiNpaSplitCompleted

Recovery

No action required.

14178 - NPA Split completed

Event Type	PROV
Description	NPA Split completed.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvNpaSplitCompleted

Recovery

No action required for this event.

14200 - Failed to initialize PDE task

Alarm Group:	PDE
Description:	The application failed to initialize the PDE task.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeInitFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Tekelec HLR Router > PDE > Options**.
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14201 - PDE failed to collect performance data

Alarm Group:	PDE
Description:	Performance data was not collected by PDE.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeCollectionFailedNotify

Recovery

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

14202 - PDE failed to generate report in CSV format

Alarm Group:	PDE
Description:	The PDE has failed to generate a report in CSV format.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeGenerationFailedNotify

Recovery

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

14203 - PDE failed to transfer CSV file

Alarm Group:	PDE
Description:	The PDE has failed to transfer the CSV file.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeTransferFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Tekelec HLR Router > PDE > Options**.
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14210 - Failed to initialize Key Exchange for PDE

Alarm Group:	PDE
Description:	The key exchange for PDE has failed to initialize.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeKeyExchInitFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Tekelec HLR Router > PDE > Options**.
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14211 - Failed to exchange keys for PDE

Alarm Group:	PDE
Description:	The key exchange for PDE has failed.
Severity:	Minor

Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeKeyExchangeFailedNotify

Recovery

1. Log into the primary NOAM.
2. Select **Tekelec HLR Router > PDE > Options**.
3. Replace the existing PDE options and click **Apply**.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14212 - Failed to delete password from PDE Options table

Alarm Group:	PDE
Description:	The password was not deleted from the PDE Options table.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autoclear.
OID	eagleXgHlrRouterPdeDeletePasswordFailedNotify

Recovery

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

14230 - PDE successful

Event Type:	PDE
Description:	This event is generated each time a PDE task is successfully completed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	86400
OID:	eagleXgHlrRouterPdeAgentSuccessNotify

Recovery

Informational event; no action required.

14231 - PDE Key Exchange successful

Event Type:	PDE
Description:	This event is generated each time a PDE key exchange is successfully completed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	86400
OID:	eagleXgHlrRouterPdeKeyExchangeSuccessNotify

Recovery

Informational event; no action required.

14301 - ERA Responder failed

Alarm Group:	ERA
Description:	The event responder failed.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds	This alarm does not autclear.
OID	eagleXgHlrRouterEraResponderFailedNotify

Recovery

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

14400 - Default value not configured in ExhrOptions table

Alarm Group:	SIG
Description:	Asserted when the 'exhr' process attempts to use a default value that is not configured.
Severity:	Major
Instance:	Name of default value in ExhrOptions table
HA Score:	Normal
Auto Clear Seconds:	5
OID:	eagleXgHlrRouterSigDefaultValueNotConfiguredNotify

Recovery

1. Log into the primary NOAM.

2. Select **Tekelec HLR Router > Configuration > Options** and configure the following options as necessary:
 - Default Country Code
 - Default Network Destination Code
 - Default Mobile Country Code
 - Default Mobile Network Code
3. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14401 - Service config entry not configured

Alarm Group:	SIG
Description:	Asserted when the 'exhr' process attempts to find a ServiceConfig entry for a TT/SSN pair that is not configured.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	5
OID:	eagleXgHlrRouterSigServiceConfigEntryNotConfiguredNotify

Recovery

1. Log into the primary NOAM.
2. Select **Tekelec HLR Router > Configuration > Service Config**.
3. **Edit** an existing, or **Insert** a new, service configuration.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14402 - Number trans entry not configured

Alarm Group:	SIG
Description:	Asserted when the 'exhr' process attempts to find a NumberTrans entry for a CC/NDC that is not configured.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	5
OID:	eagleXgHlrRouterSigNumberTransEntryNotConfiguredNotify

Recovery

1. Log into the primary NOAM.
2. Select **Tekelec HLR Router > Configuration > Substitutions**.
3. **Edit** an existing, or **Insert** a new, substitution.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14403 - Exception entry not configured

Alarm Group:	SIG
Description:	Asserted when the 'exhr' process attempts to find an Exception entry for a TT/NP/DPC tuple that is not configured.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	5
OID:	eagleXgHlrRouterSigExceptionEntryNotConfiguredNotify

Recovery

1. Log into a SOAM.
2. Select **Tekelec HLR Router > Configuration > Exception Routing**.
3. Click **Edit** to edit an existing exception or click **Insert** to insert a new exception.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14405 - Invalid CdPA GTI

Event Type:	SIG
Description:	The Called Party Global Title Indicator is invalid.
Severity:	Info
Instance:	GTI
HA Score:	Normal
Throttle Seconds:	5
OID:	eagleXgHlrRouterSigInvalidCdpaGtiNotify

Recovery

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

14406 - Cannot route to Network Entity

Event Type:	SIG
Description:	Data cannot be routed to the Network Entity.
Severity:	Info
Instance:	Network Entity
HA Score:	Normal

Throttle Seconds: 5
OID: eagleXgHlrRouterSigCannotRouteToNetworkEntityNotify

Recovery

1. Log into the active NOAM.
2. Select **EAGLE XG Database > Configuration > Network Entity**.
3. Click the **Update** tab.
4. Look up the relevant Network Entity and fix the Network Entity's configuration.
5. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14407 - Mate not configured

Event Type: SIG
Description: The mated network entity is not configured.
Severity: Info
Instance: Network Entity
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgHlrRouterSigMateNotConfiguredNotify

Recovery

1. Log into the active NOAM.
2. Select **Tekelec HLR Router > Configuration > Mated Entities**.
3. Insert a new Network Entity mate configuration.
4. If the problem persists, it is recommended to contact [My Oracle Support \(MOS\)](#).

14408 - MP E164 Not Configured

Event Type: SIG
Description: MP E164 is not configured.
Severity: Info
Instance: E.164 Address
HA Score: Normal
Throttle Seconds: 5
OID: eagleXgHlrRouterSigMpE164NotConfiguredNotify

Recovery

1. Log into the active SOAM.
2. Select **Tekelec HLR Router > Configuration > MP E.164**.
3. Insert a new E.164 address to assign to an MP.

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

SS7/Sigtran Alarms (19200-19299)

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

19200 - RSP/Destination unavailable

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

Recovery:

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

19201 - RSP/Destination route unavailable

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

OID: awpss7M3rlRouteUnavailableNotify

Recovery:

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

19202 - Linkset unavailable

Alarm Group: SS7

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

Severity: Major

Instance: <LinkSetName>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlLinksetUnavailableNotify

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link set status can be monitored from **SS7/Sigtran > Maintenance > Linksets**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact [My Oracle Support \(MOS\)](#).

19203 - Link unavailable

Alarm Group: SS7

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

Severity: Minor

Instance: <Link Name>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlLinkUnavailableNotify

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link status can be monitored from **SS7/Sigtran > Maintenance > Links**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact [My Oracle Support \(MOS\)](#).

19204 - Preferred route unavailable

Alarm Group:	SS7
Description:	M3RL has started to utilize a lower priority (higher cost) route to route traffic toward a given destination address, because the higher priority (lower cost) route specified for that RSP/Destination has become Unavailable.
Severity:	Major
Instance:	RSP Name
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7M3rlPreferredRouteUnavailableNotify

Recovery:

1. If the preferred route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Route status can be monitored from **SS7/Sigtran > Maintenance > Remote Signaling Points**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, 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:	awpss7M3rlTfcReceivedNotify

Recovery:

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

19209 - M3RL routing error

Event Type:	SS7
Description:	A message was discarded due to a routing error.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	10
OID:	awpss7M3rlRoutingFailureNotify

Recovery:

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

19212 - CFG-DB Validation Error

Alarm Group:	SS7
Description:	A minor database validation error was detected on the MP server during an update. MP internal database is not 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)
Throttle Seconds	86,400 seconds
OID	awpss7CfgDbValidationErrorNotify

Recovery:

1. An unexpected condition had occurred while performing a database update. Because the nature of the error was not critical, database updates are still enabled, but this error should be investigated as soon as possible.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

19213 - CFG-DB Update Failure

Alarm Group:	SS7
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)
Throttle Seconds	86,400 seconds
OID	awpss7CfgDbUpdateFailureNotify

Recovery:

1. An unexpected condition had occurred while performing a database update. Because the nature of the error was critical, database updates are now disabled.

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

19214 - CFG-DB post-update Error

Alarm Group:	SS7
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)
Throttle Seconds	86,400 seconds
OID	awpss7CfgDbPostUpdateErrorNotify

Recovery:

1. An unexpected condition has occurred while performing a database update. Because the nature of the error was not critical, database updates are still enabled, but this error should be investigated as soon as possible.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

19215 - CFG-DB post-update Failure

Alarm Group:	SS7
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)
Throttle Seconds	86,400 seconds
OID	awpss7CfgDbPostFailureNotify

Recovery:

1. An unexpected condition has occurred while performing a database update. Because the nature of the error was critical, database updates are now disabled.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

19216 - Measurement Initialization Failure

Alarm Group:	SS7
Description:	A measurement object failed to initialize.
Severity:	Critical
Instance:	<measTagName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
Throttle Seconds	86,400 seconds
OID	awpss7MeasurementInitializationFailureNotify

Recovery:

1. Measurement subsystem initialization has failed for the specified measurement.
2. It is recommended to contact [My Oracle Support \(MOS\)](#).

19217 - Node isolated - all links down

Alarm Group:	SS7
Description:	All configured links are down; either failed or disabled. No M3UA signaling is possible. The node is isolated from the network. All M3UA connectivity to the SS7/Sigtran network has either failed or has been manually disabled.
Severity:	Critical
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7M3r1NodeIsolatedAllLinkDownNotify

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:	30
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.
HA Score:	Normal

Throttle Seconds: 10
OID: awpss7ReceivedInvalidM3uaMessageNotify

Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the malformed message.
 - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
 - Error code 0x03 indicates an unsupported M3UA message class.
 - Error code 0x04 indicates an unsupported M3UA message type.
 - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
 - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
 - Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
 - Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
 - Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
 - Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.
2. If the problem persists, 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: awpss7FailedToSendNonDataMessageNotify

Recovery:

1. Select **Alarms & Events > View History** and check the event history logs for additional SS7 events or alarms from this MP server.
2. Verify that the adjacent server on the Signaling Gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.
3. If the problem persists, 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 \(MOS\)](#).

19240 - Remote SCCP subsystem prohibited

Alarm Group:	SS7
Description:	The status of remote SCCP subsystem has changed to Prohibited .
Severity:	Minor
Instance:	<RMU>
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7RemoteSccpSubsystemProhibitedNotify

Recovery:

1. You can monitor destination status from **SS7/Sigtran > Maintenance > Remote Signaling Points** and RMU/subsystem status from **SS7/Sigtran > Maintenance > Remote MTP3 Users**.
 - If the subsystem's status changed to **Prohibited** because SCMG received a SSP message, an audit of the status of the RMU via the SCCP subsystem status test (SST) procedure is performed.
 - If the subsystem's status changed to **Prohibited** because SCCP received a MTP-PAUSE indication from M3RL, then recovery actions of restoring the RSP/Destination status to **Available** will be invoked by M3RL.
 - If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS cause=unequipped user indication from M3RL, then no automatic recovery will be initiated.

Only manual action at the remote node can correct a remote point code that has not been configured with SCCP.

- If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS cause=unknown or inaccessible indication from M3RL, then SCCP will automatically invoke subsystem status testing depending upon the network type:
 - ANSI: subsystem status testing of all RMUs associated with the point code.
 - ITU: subsystem status testing SCMG (SSN=1) associated with the point code.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
 3. Select **Alarms & Events > View History** and check the event history logs for additional SS7 events or alarms from this MP server.
 4. Verify 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 malformed or unsupported message

Event Type:	SS7
Description:	SCCP discarded an ingress message because the Message Type is not currently supported. The following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. The following SCMG Message Types are supported: SSA, SSP, and SST.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	30
OID:	awpss7SccpMsgTypeUnrecognizedNotify

Recovery:

1. Investigate:
 - If the originator of the message is misconfigured.
 - If the network is misconfigured, causing messages to be routed to the wrong RSP/Destination.
 - If the message type is currently unsupported.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

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 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 message during SCCP processing due to transient conditions such as RSP/destination failures and remote or local subsystem failures.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	30

OID: awpss7SccpRoutingFailureNetworkStatusNotify

Recovery:

1. Monitor status on the GUI main menu as follows:
 - Destination status from **SS7/Sigtran > Maintenance > Remote Signaling Points**.
 - RMU/subsystem status from **SS7/Sigtran > Configuration > Remote MTP3 Users**.
 - Local subsystem status from **SS7/Sigtran > Maintenance > Local SCCP Users**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, 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
HA Score:	Normal
Throttle Seconds:	10
OID:	awpss7SccpGttFailureNotify

Recovery:

1. Global title translation has failed. For the cause of the failure, look at the SCCP return cause and the called party address information in the event additional information field. Look for the following items:
 - Missing global title translation data.
 - Incorrect called party address information in the ingress message.
 - Point code paused or congested.
 - Subsystem prohibited or congested.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

19246 - Local SCCP subsystem prohibited

Alarm Group:	SS7
Description:	The status of the local SCCP subsystem has changed to Prohibited . This alarm is raised for one of the following conditions: <ul style="list-style-type: none"> • 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 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:

- On the SOAM GUI main menu, select **SS7/Sigtran > Configuration > Local SCCP Users**.
- 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.
- Click **Enable** to put the appropriate local SSN in the enabled state.
A confirmation message appears.
- Click **OK**.

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

19248 - SCCP Segmentation Failure

Event Type: SS7
Description: SCCP Segmentation Procedure Failure
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 30
OID: awpss7SccpSegmentationFailureNotify

Recovery:

- This condition indicates segmentation procedure failure at the SCCP layer:
 - User data exceeds maximum size
 - Internal Error
- Check the SCCP options configuration and maximum size limitations for the SS7 network.
- Contact the [My Oracle Support \(MOS\)](#) for assistance.

19249 - SCCP Reassembly Failure

Event Type:	SS7
Description:	SCCP Reassembly Procedure Failure
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	30
OID:	awpss7SccpReassemblyFailureNotify

Recovery:

1. This condition indicates reassembly procedure failure at the SCCP layer:
 - Reassembly time expired
 - Out of sequence segments
 - Internal error
2. Determine if the problem is a result of routing decision errors or latency from the SS7 network.
3. Contact the [My Oracle Support \(MOS\)](#) for assistance.

19250 - SS7 process CPU utilization

Alarm Group:	SS7
Description:	The SS7 process, which is responsible for handling all SS7 traffic, is approaching or exceeding its engineered traffic handling capacity.
Severity:	Minor, Major, or Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7Ss7ProcessCpuUtilizationNotify

Recovery:

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

4. The SS7 process may be experiencing problems. You monitor the alarm log from **Alarms & Events > View Active**.
5. If the problem persists, contact [My Oracle Support \(MOS\)](#).

19251 - Ingress message rate

Alarm Group:	SS7
Description:	The ingress message rate (messages per second) for the MP is approaching or exceeding its engineered traffic handling capacity.
Severity:	Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7IngressMsgRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from 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 Group:	SS7
Description:	The percent utilization of the MP's PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded.
Severity:	Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	<PoolName> Values: ANSI, ITUI, ITUN
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7PduBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from 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 Group:	SS7
Description:	The percent utilization of the MP's SCCP stack event queue is approaching its maximum capacity.
Severity:	Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7SccpStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from 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 Group:	SS7
---------------------	-----

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from 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 Group:	SS7
Description:	The percent utilization of the MP's M3RL Network Management Event Queue is approaching its maximum capacity.
Severity:	Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7M3rlNetMgmtEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from 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 Group:	SS7
Description:	The percent utilization of the MP's M3UA Stack Event Queue is approaching its maximum capacity.
Severity:	Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7M3uaStackEventQueueUtilNotify

Recovery:

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

19258 - SCTP Aggregate Egress queue utilization

Alarm Group:	SS7
Description:	The percent utilization of events queued to all SCTP associations on the MP server is approaching maximum capacity.
Severity:	Minor, Major, Critical as shown in the GUI under Alarms & Events > View Active .
Instance:	N/A

HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7SctpAggregateAssocWriteQueueUtilNotify

Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events > View Active**.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from 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
 - the SCCP called party address to which the message was destined if the component was ever sent
3. Check for SCCP events just prior to this event indicating that a message could not be routed. If SCCP failed to route the message, verify that a route exists for the destination to which the TCAP message was being sent.
4. If no SCCP routing failure event exists, investigate why the remote TCAP peer failed to respond. The DPC and called party address (if present) can be used to determine the destination to which the message was being sent.
5. If the DPC and Called Party Address are not included in the additional information field, it indicates that the component was created, but never sent.
6. 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 Group:	SS7
Description:	TCAP active dialogue utilization
Severity:	Minor, Major, Critical
Instance:	Application name
HA Score:	Normal
Auto Clear Seconds:	0 (alarm does not clear automatically)
OID:	awpss7TcapActiveDialogueUtilNotify

Recovery:

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

19273 - TCAP active operation utilization

Alarm Group:	SS7
Description:	TCAP active operation utilization
Severity:	Minor, Major, Critical

Instance:	Application name
HA Score:	Normal
Auto Clear Seconds:	0 (alarm does not clear automatically)
OID:	awpss7TcapActiveOperationUtilNotify

Recovery:

1. The percent utilization of the MP's component table is approaching maximum capacity. This alarm indicates that the number of active egress TCAP operations on the MP server is higher than expected.
2. If this problem persists and the component table reaches 100% utilization, all new egress operations will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This may be caused by any of the following:
 - the outgoing rate of new operations is higher than expected (possibly due to a higher than expected average number of operations per message)
 - the duration of the operations is longer than expected
 - both the outgoing rate and duration are higher than expected
 - a software problem is preventing removal of components
3. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

19274 - TCAP stack event queue utilization

Alarm Group:	SS7
Description:	TCAP stack event queue utilization
Severity:	Minor, Major, Critical
Instance:	Application name
HA Score:	Normal
Auto Clear Seconds:	0 (alarm does not clear automatically)
OID:	awpss7TcapStackEventQueueUtilNotify

Recovery:

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

Transport Manager Alarms and Events (19400-19499)

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

19400 - Transport Down

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

Recovery:

1. The Active alarm instance data, which can be viewed from **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 Group: TMF
Description: Received malformed SCTP message (invalid length)
Severity: Info
Instance: <TransportName>

HA Score: Normal
Throttle Seconds: 0 (zero)
OID: awptransmgrReceivedMalformedTransSctpMessageNotify

Recovery:

1. An SCTP message was received containing a message not valid in length.
2. If the alarm persists, contact [My Oracle Support \(MOS\)](#).

19404 - Far-end closed the Transport

Event Type: TMF
Description: Far-end closed the Transport
Severity: Info
Instance: <TransportName>
HA Score: Normal
Throttle Seconds: 10
OID: awptransmgrFarEndClosedTheTransportNotify

Recovery:

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

To Troubleshoot:

- Investigate the adjacent node at the specified IP address and port to determine if it failed or if it is under maintenance.
 - Check the adjacent node for alarms or logs that might indicate the cause for their closing the association.
2. If the alarm persists, 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:	awpransmgrLocalTransportMaintenanceStateChangeNotify

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 \(MOS\)](#).

19408 - Single Transport Egress-Queue Utilization

Alarm Group:	TMF
Description:	The percent utilization of the MP's single Transport Egress-Queue is approaching its maximum capacity
Severity:	Based on defined Thresholds. Minor, Major, Critical Engineered Max Value = 1000
Instance:	<TransportName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	awptransmgrTransSingleWriteQueueUtilNotify

Recovery:

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

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

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

- If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. MP server status can be monitored from **Main Menu > Status & Control > Server Status**.
 - The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
 - There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Main Menu > Status & Control > KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
2. If the alarm persists, 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:	10
OID:	awptransmgrMessageRejectedByAclFilteringNotify

Recovery:

1. Verify that the ENUM server's IP address is the ACL, or that the ACL is empty.
2. If the alarm persists, 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>, <TransportId>
HA Score:	Normal
Throttle Seconds:	0 (zero)
OID:	awptransmgrSctpTransportRefusedNotify

Recovery:

1. Recheck the Adjacent Node's configure IP Address and validation mode.
2. If alarm persists, contact [My Oracle Support \(MOS\)](#).

19412 - SCTP Transport configuration mismatched for Adjacent Node IP

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

Recovery:

1. Recheck the Configured IP Address and Transport configuration and validation mode.
2. If the alarm persists, contact [My Oracle Support \(MOS\)](#).

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

Alarm Group:	TMF
Description:	SCTP Transport closed due to unsupported add/delete peer IP Address event recieved in Peer Address Notification
Severity:	Info
Instance:	<TransportName>
HA Score:	Normal
Throttle Seconds:	0 (zero)

OID: awptransmgrTransportClosedDueToUnsupportedEventNotify

Recovery:

1. Disable SCTP Dynamic Address Reconfiguration at the Adjacent Node.
2. If the alarm persists, 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 **Alarms & Events > View Active** GUI menu option. The alarms and events log can be viewed from the **Alarms & Events > View History** page.

19800 - Communication Agent Connection Down

Alarm Group: CAF

Description: This alarm indicates that a Communication Agent is unable to establish transport connections with one or more other 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 Group: CAF

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

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

Severity: Minor

Instance: N/A

Note: This alarm is cleared when:

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnLocalBlockedNotify

Recovery:

1. Use **Main Menu > Alarms & Events > View History** to find additional information about the alarm.

The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.

2. Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Main Menu > Communication Agent > Maintenance > Connection Status** to determine which connections on the server have abnormal status.
4. If the expected set of connections is locally blocked, then no further action is necessary.
5. To remove a the local block condition for a connection, use the **Main Menu > Communication Agent > Maintenance > Connection Status** screen and click the 'Enable' action button for the desired connection.
6. Contact [My Oracle Support \(MOS\)](#) for assistance.

19802 - Communication Agent Connection Remotely Blocked

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

Note: This alarm is cleared when:

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnRemoteBlockedNotify

Recovery:

1. Use **Main Menu > Alarms & Events > View History** to find additional information about the alarm.

The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.

2. Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Main Menu > Communication Agent > Maintenance > Connection Status** to determine which connections on the server have abnormal status.
4. If the expected set of connections is locally blocked, then no further action is necessary.
5. To remove a the local block condition for a connection, use the **Main Menu > Communication Agent > Maintenance > Connection Status** screen and click the 'Enable' action button for the desired connection.
6. Contact *My Oracle Support (MOS)* for assistance.

19803 - Communication Agent stack event queue utilization

Alarm Group: CAF

Description:	The percent utilization of the Communication Agent Task stack queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded, based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode.
Severity:	Minor, Major, Critical
Instance:	<ComAgent StackTask Name>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFQueueUtilNotify

Recovery:

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

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

Contact [My Oracle Support \(MOS\)](#) for assistance.

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

Alarm Group:	CAF
Description:	Communication Agent configured connection waiting for remote client to establish connection. This alarm indicates that a Communication Agent is waiting for one or more far-end client MPs to initiate transport connections. Generally this alarm is asserted when a client MP or the IP network is undergoing maintenance or when a connection has been manually disabled at a client MP. Note: It is normal to have this auto-clearing connection alarm for the remote server connections that configured manually in "Client" mode, but are not yet available for processing traffic.
Severity:	Minor

Instance: N/A

Note: The alarm is cleared when a "server" connection exits the "forming" state and no other connection having "server" connect mode is in the "forming" state or the auto-clear time-out occurs.

- The MP Server/Connection is deleted
- When connection is moved to TotallyBlocked/RemotelyBlocked/InService state from Aligning
- Auto Clear
- Connection is disabled

HA Score: Normal

Auto Clear Seconds: 300 (5 min)

OID: cAFClientConnWaitNotify

Recovery:

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

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

- The MP Server/Connection is deleted
 - When connection is moved to TotallyBlocked/RemotelyBlocked/InService state from Aligning
 - Auto Clear
 - Connection is disabled
2. Check the event history logs at **Main Menu > Alarms & Events > View History** for additional Communication Agent events or alarms from this MP server.
 3. Check **Main Menu > Communication Agent > Maintenance > Connection Status** to determine which connections on the server have abnormal status.
 4. Verify that the remote server is not under maintenance.
 5. If the connection is manually disabled at the client MP, and it is expected to be disabled, then no further action is necessary.
 6. If the connection has been manually disabled at the client MP, but it is not supposed to be disabled, then enable the connection by clicking on the 'Enable' action button on the Connection Status screen.
 7. Verify that IP network connectivity exists between the two connection end-points.
 8. Verify that the connection's local IP address and port number are configured on remote client MP.
 9. Verify that the Application Process using Communication Agent plug-in is running on both ends.
 10. Verify that the connection's remote IP address and port correctly identify remote's listening port.
 11. Contact [My Oracle Support \(MOS\)](#) for assistance.

19805 - Communication Agent Failed To Align Connection

Alarm Group: CAF

Description:	The Communication Agent failed to align connection. This alarm indicates that Communication Agent has established one or more transport connections with servers that are running incompatible versions of software, and so Communication Agent is unable to complete the alignment of the connection. A connection that fails alignment cannot be used by applications to communicate with other servers, and so this alarm may indicate that applications are unable to communicate with their expected set of peers.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFConnAlignFailedNotify

Recovery:

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

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

6. Contact [My Oracle Support \(MOS\)](#) for assistance.

19806 - Communication Agent CommMessage mempool utilization

Alarm Group:	CAF
Description:	<p>The percent utilization of the Communication Agent CommMessage mempool is approaching defined threshold capacity.</p> <p>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.</p>
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 ingres 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 Group: CAF

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

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFUserDataFIFOutilNotify

Recovery:

1. 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 Group:	CAF
Description:	The percent utilization of the Communication Agent Connection FIFO Queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new ComAgent internal Connection Management StackEvents messages can be discarded based on Application's Global Congestion Threshold Enforcement Mode.
Severity:	Minor, Major, Critical
Instance:	<ComAgent StackTask Name>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFMxFIFOUtilNotify

Recovery:

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

19810 - Communication Agent Egress Message Discarded

Event Type:	CAF
Description:	The Communication Agent egress message is being discarded due to one of the following reasons: <ul style="list-style-type: none"> • Unknown destination server • Connection state is not InService • Incompatible destination • Serialization failed • MxEndpoint send failed • Internal error
Severity:	Info
Instance:	<RemoteIP> <p>Note: If <RemoteIP> is not known at the time of message discard, then "Unknown" will be used.</p>
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
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: <RemoteIP>
HA Score: Normal
OID: cAFEventConnectionStateChangeNotify

Recovery:

1. Use **Main Menu > Alarms & Events** and examine the alarm log.
This Event is a log of connection state change.
2. Contact [My Oracle Support \(MOS\)](#) for assistance.

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

Event Type:	CAF
Description:	Communication Agent DB Responder detected a change in configurable control option parameter. Note: This event is an indication that Communication Agent detected a control parameter change. The change will be applied to applicable software component. If the change is applied on the GUI, the appropriate GUI action is logged in security logs. If the action is not performed from GUI and the control parameter is changed, this event indicates the executed change.
Severity:	Info
Instance:	N/A
HA Score:	Normal
OID:	cAFEventComAgtConfigParamChangeNotify

Recovery:

1. Use **Main Menu > Alarms & Events** and examine the alarm log.
2. Use **Main Menu > Security Log** and examine the alarm log.
3. If the event shows up in **Main Menu > Alarms & Events**, without the corresponding GUI security-log in **Main Menu > Security Log**. Contact [My Oracle Support \(MOS\)](#) for assistance.

19818 - Communication Agent DataEvent Mempool utilization

Event Type:	CAF
Description:	The percent utilization of the Communication Agent DataEvent Mempool is approaching defined threshold capacity.
Severity:	Minor, Major, Critical
Instance:	<ComAgent Process>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFDataEvPoolResUtilNotify

Recovery:

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

19820 - Communication Agent Routed Service Unavailable

Alarm Group:	CAF
Description:	This alarm indicates that all connections of all connection groups associated with a Routed Service are unavailable. This generally occurs when far-end servers have been removed from service by maintenance actions. This can also occur if all of the Routed Service's connections have been either disabled or blocked.
Severity:	Major
Instance:	<RoutedServiceName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFRSUnavailNotify

Recovery:

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

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

4. Contact [My Oracle Support \(MOS\)](#) for assistance.

19821 - Communication Agent Routed Service Degraded

Alarm Group:	CAF
Description:	This alarm indicates that some, but not all, connections are unavailable in the connection group being used by a Communication Agent Routed Service to route messages. The result is that the server that posted this alarm is not load-balancing traffic across all of the connections configured in the connection group.
Severity:	Major
Instance:	<ServiceName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFRSDegradedNotify

Recovery:

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

2. Use **Main Menu > Communication Agent > Maintenance > Connection Status** to view the reasons why connections are unavailable.
3. Use **Main Menu > Status & Manage > Server** to confirm that the far-end servers have an application state of enabled, and that their subsystems are operating normally.

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

4. Contact [My Oracle Support \(MOS\)](#) for assistance.

19822 - Communication Agent Routed Service Congested

Alarm Group:	CAF
Description:	This alarm indicates that a routed service is load-balancing traffic across all connections in a connection group, but all of the connections are experiencing congestion. Messages may be discarded due to congestion.
Severity:	Major
Instance:	<ServiceName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFRSCongestedNotify

Recovery:

1. Use **Main Menu > Communication Agent > Maintenance > Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Main Menu > Communication Agent > Maintenance > Connection Status** to view the are congested and the degree to which they are congested.
3. Check the far-end of the congested connections in order to further isolate the cause of congestion.
If the far-end servers are overloaded, then it is possible that the system is being presented a load that exceeds its engineered capacity. If this is the case, then either the load must be reduced, or additional capacity must be added.
4. Contact [My Oracle Support \(MOS\)](#) for assistance.

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

Alarm Group:	CAF
Description:	Communication Agent routed service is routing traffic using a connection group that has a lower-priority than another connection group.
Severity:	Major
Instance:	<ServiceName>
HA Score:	Normal

Auto Clear Seconds: 0 (zero)
OID: cAFRSUsingLowPriConnGrpNotify

Recovery:

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

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

4. Contact [My Oracle Support \(MOS\)](#) for assistance.

19824 - Communication Agent Pending Transaction Utilization

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

Recovery:

1. 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 Group: CAF

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

Recovery:

1. 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 Group:	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 overloaded 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
OID:	cAFEventComAgtSvcRegChangedNotify

Recovery:

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

19831 - Communication Agent Service Operational State Changed

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

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> <ul style="list-style-type: none"> • 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> <ul style="list-style-type: none"> • 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
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
Instance:	<ProviderServerName>: <ResourceName>
HA Score:	Normal
OID:	cAFEventResourceStateChangeNotify
Recovery:	No action required.

19844 - Communication Agent Resource-Provider Stale Status Received

Event Type:	CAF
Description:	Communication Agent Resource-Provider Stale Status Received.
Severity:	Info
Instance:	<ProviderServerName>: <ResourceName>
HA Score:	Normal
Throttle Seconds:	10

OID: cAFEventStaleHBPacketNotify

Recovery:

If this event is occurring frequently then check the ComAgent maintenance screens for other anomalies and to troubleshoot further.

19845 - Communication Agent Resource-Provider Deregistered

Event Type: CAF
Description: Communication Agent Resource-Provider Deregistered.
Severity: Info
Instance: <ResourceName>
HA Score: Normal
OID: cAFEventResourceProviderDeRegisteredNotify

Recovery:

No action required.

19846 - Communication Agent Resource Degraded

Alarm Group: CAF
Description: Communication Agent Resource Degraded. A local application is using the resource, identified in the alarm, and the access to the resource is impaired. Some of the resource providers are either unavailable and/or congested.
Severity: Major
Instance: <ResourceName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: cAFResourceCongestedNotify

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 Group: CAF

Description:	Communication Agent Resource Unavailable. A local application needs to use a ComAgent resource, but the resource is unavailable. The resource can be unavailable if the local server has no ComAgent connections to servers providing the resource or no servers host active instances of the resource's sub-resources.
Severity:	Major
Instance:	<ResourceName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFResourceUnavailNotify

Recovery:

1. 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 Group:	CAF
Description:	Communication Agent Resource Error. Two sets of servers are using incompatible configurations for a ComAgent resource.
Severity:	Minor
Instance:	<ResourceName>
HA Score:	Normal
Auto Clear Seconds:	50
OID:	cAFResourceErrorNotify

Recovery:

1. Use **Main Menu > Communication Agent > Maintenance > HA Services Status** to determine which sets of servers are incompatible.

Check the incompatible servers to verify that they are operating normally and are running the expected versions of software.
2. 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
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
OID:	cAFEventResourceUserDeRegisteredNotify
Recovery:	No action required.

19852 - Communication Agent Resource Routing State Changed

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

19853 - Communication Agent Resource Egress Message Discarded

Event Type:	CAF
Description:	Communication Agent Resource Egress Message Discarded.

Severity:	Info
Instance:	<ResourceName>: <SubResourceID>
	Note: If the resource is unknown, then <ResourceName> is the ResourceID converted to text. The <SubResourceID> is an integer converted to text, regardless of whether it is known or unknown.
HA Score:	Normal
Throttle Seconds:	10
OID:	cAFEventHaEgressMessageDiscardedNotify

Recovery:

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

If the condition is persistent with the status of one of the ComAgent Configuration Managed Objects there is an underlying issue with the Managed Object.

2. Use **Main Menu > Alarms & Events** and examine the alarm log for ComAgent Process problems.
3. Contact [My Oracle Support \(MOS\)](#) for assistance.

19854 - Communication Agent Resource-Provider Tracking Table Audit Results

Event Type:	CAF
Description:	Communication Agent Resource-Provider Tracking Table Audit Results. This event is generated when a Resource Provider Tracking Table (RPTT) entry with Status equal to Auditing is replaced with a new status (null, Active, Standby, Spare, OOS, etc) and there are no other RPTT entries, for this specific Resource/SR, with Status equal to Auditing.
Severity:	Info
Instance:	None
HA Score:	Normal
OID:	cAFEventHaRPTTAuditResultNotify

Recovery:

No action required.

19855 - Communication Agent Resource Has Multiple Actives

Alarm Group:	CAF
Description:	This alarm indicates a possible IP network disruption that has caused more than one Resource Provider to become Active. The server that asserted this alarm expects there to be only one active Resource Provider server for the Resource, but instead it is seeing more than one. During this condition the server may be sending commands to the wrong Resource Provider. This may affect applications such as CPA, PDRA.
Severity:	Major

Instance: <ResourceName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: cAFMultipleActivesNotify

Recovery:

1. Use **Main Menu > Communication Agent > Maintenance > HA Services Status** to determine which Resource Provider servers are announcing 'Active' status for the Resource.
2. Investigate possible IP network isolation between these Resource Provider servers.
3. 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
OID: cAFEEventSvcProvRegStateChangedNotify

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
OID: cAFEEventSvcProvOpStateChangedNotify

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 \(MOS\)](#).

19858 - Communication Agent Connection Rejected

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

Recovery:

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

19860 - Communication Agent Configuration Daemon Table Monitoring Failure

Alarm Group:	CAF
Description:	This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.
Severity:	Critical
Instance:	None
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFTableMonitorFailureNotify

Recovery:

1. Use **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 Group:	CAF
Description:	This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.
Severity:	Critical
Instance:	None
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	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:	<ul style="list-style-type: none"> • Minor - if exceeding 100K on Gen8/Gen9 hardware, 75k on other hardware • Major - if exceeding 110K on Gen8/Gen9 hardware, 80k on other hardware

- Critical - if exceeding 120K on Gen8/Gen9 hardware, 84k on other hardware

Instance: <ServiceName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: cAFIngressRateNotify

Recovery:

1. This alarm indicates that a server is overrunning its defined processing capacity. If any of the defined threshold onset levels are exceeded, Communication Agent will discard comparatively low priority messages. Check the configuration, routing, and deployment mode capacity.
2. 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: 10
OID: cAFComAgentMaxConnsInConnGrpNotify

Recovery:

1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.
2. 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
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
OID:	cAFEventFailToSetHostServerHWProfileNotify

Recovery:

1. This event indicates that there is a failure in applying default hardware settings for ComAgent TPS controlling parameters. When default settings also fail to apply, then the factory values will be used for the TPS controlling parameters.
2. If needed, contact [My Oracle Support \(MOS\)](#).

19866 - Communication Agent Peer Group Status Changed

Event Type:	CAF
Description:	The Communication Agent Peer Group operational status has changed
Severity:	Info
Instance:	<PeerGroupName>
HA Score:	Normal
OID:	cAFEventPeerGroupStatusChangeNotify

Recovery:

This alarm is informational and no action is required.

19867 - Communication Agent Peer Group Egress Message Discarded

Event Type:	CAF
Description:	The Communication Agent Peer Group egress message is being discarded due to one of the following reasons: <ul style="list-style-type: none"> • Unknown Peer Group • Peer Group Unavailable • Peer Congested • Reliability not supported

Severity:	Info
Instance:	<PeerGroupName>
HA Score:	Normal
Throttle Seconds:	10
OID:	cAFEventPSEgressMessageDiscardedNotify

Recovery:

This alarm is informational and no action is required.

19868 - Communication Agent Connection Rejected - Incompatible Network

Event Type:	CAF
Description:	Communication Agent connection rejected. Connection to the peer node is not initiated due to network incompatibility. This event will be raised on the connection initiator side when the connection initiator MP has only IPv6 IP addresses configured and Remote MP has only IPv4 IP addresses configured or when connection initiator MP has only IPv4 IP addresses configured and Remote MP has only IPv6 IP addresses configured.
Severity:	Info
Instance:	<RemoteIP>
HA Score:	Normal
OID:	cAFEventConnectionRejectNotify

Recovery:

1. Disable both sides of the connection.
2. Configure the correct network modes on either server.
3. Restart the application on the reconfigured server.
4. Enable both sides of the connection.
5. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

EXG Stack (19000-19999)

This section provides information and recovery procedures for EXG Stack alarms, ranging from 19000-19999.

19900 - DP Server CPU utilization

Alarm Group	STK
Description	The percent utilization of the DP Server CPU is approaching its maximum capacity.

Severity	<ul style="list-style-type: none"> • Minor when utilization exceeds 60%. • Major when utilization exceeds 66%. • Critical when utilization exceeds 72%.
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID	dbcProcessCpuUtilizationNotify

Recovery

The alarm will clear when utilization falls below the established threshold.

- Minor alarm clears when utilization falls below 57%.
- Major alarm clears when utilization falls below 63%.
- Critical alarm clears when utilization falls below 69%.

19901 - CFG-DB Validation Error

Alarm Group:	STK
Description:	A minor database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are ALLOWED.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	dbcCfgDbValidationErrorNotify

Recovery:

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

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

Recovery:

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 Group:	STK
Description:	A minor database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are ALLOWED.
Severity:	Major
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	dbcCfgDbPostUpdateErrorNotify

Recovery:

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 Group:	STK
Description:	A critical database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are DISABLED.
Severity:	Critical
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	dbcCfgDbPostFailureNotify

Recovery:

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

Contact [My Oracle Support \(MOS\)](#) for assistance.

19905 - Measurement Initialization Failure

Alarm Group:	STK
Description:	A measurement object failed to initialize.
Severity:	Critical
Instance:	<measTagName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	dbcMeasurementInitializationFailureNotify

Recovery:

Measurement subsystem initialization has failed for the specified measurement.

Contact [My Oracle Support \(MOS\)](#) for assistance.

19910 - Message Discarded at Test Connection

Event Type:	DIAG
Description:	Normal traffic is being discarded because it is routed to an egress Test Connection. An egress Test Connection is given a normal message to be transmitted.
Severity:	Major
Instance:	<Connection name>
HA Score:	Normal
Auto Clear Seconds:	120
OID:	dbcNormalMessageDiscardedNotify

Recovery:

1. Update routing rules to exclude Test connections from being used for routing.

Normal traffic should be received and sent on non-test connections.

2. Change the hostname of the peer connected to the test connection.

The hostname of the peer connected to the test connection may be the destination host for the incoming normal traffic.

19911 - Test message discarded

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

Recovery:

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.

Platform (31000-32800)

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32700.

31000 - S/W fault

Alarm Group:	SW
Description:	Program impaired by s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolSwFaultNotify

Recovery:

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

31001 - S/W status

Alarm Group:	SW
Description:	Program status

Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolSwStatusNotify
Recovery:	No action required.

31002 - Process watchdog failure

Alarm Group:	SW
Description:	Process watchdog timed out.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolProcWatchdogFailureNotify

Recovery:

1. Alarm indicates a stuck process was automatically recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31003 - Tab thread watchdog failure

Alarm Group:	SW
Description:	Tab thread watchdog timed out
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolThreadWatchdogFailureNotify

Recovery:

1. Alarm indicates a stuck process was automatically recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31100 - Database replication fault

Alarm Group:	SW
Description:	The Database replication process is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact [My Oracle Support \(MOS\)](#).

31101 - Database replication to slave failure

Alarm Group:	REPL
Description:	Database replication to a slave Database has failed
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepToSlaveFailureNotify

Recovery:

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact [My Oracle Support \(MOS\)](#).

31102 - Database replication from master failure

Alarm Group:	REPL
Description:	Database replication from a master Database has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300

OID: comcolDbRepFromMasterFailureNotify

Recovery:

1. Indicates replication subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, contact [My Oracle Support \(MOS\)](#).

31103 - DB Replication update fault

Alarm Group: REPL

Description: Database replication process cannot apply update to DB.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepUpdateFaultNotify

Recovery:

1. This alarm indicates a transient error occurred within the replication subsystem, but the system has recovered, so no additional steps are needed.
2. If the problem persists, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31104 - DB Replication latency over threshold

Alarm Group: REPL

Description: Database replication latency has exceeded thresholds

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepLatencyNotify

Recovery:

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

31105 - Database merge fault

Alarm Group:	SW
Description:	The database merge process (inetmerge) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMergeFaultNotify

Recovery:

1. This alarm indicates a transient error occurred within the merging subsystem, but the system has recovered, so no additional steps are needed.
2. If the problem persists, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31106 - Database merge to parent failure

Alarm Group:	COLL
Description:	Database merging to the parent Merge Node has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolDbMergeToParentFailureNotify

Recovery:

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

31107 - Database merge from child failure

Alarm Group:	COLL
Description:	Database merging from a child Source Node has failed.
Severity:	Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMergeFromChildFailureNotify

Recovery:

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

31108 - Database merge latency over threshold

Alarm Group:	COLL
Description:	Database Merge latency has exceeded thresholds
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMergeLatencyNotify

Recovery:

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

31109 - Topology config error

Alarm Group:	DB
Description:	Topology is configured incorrectly
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolTopErrorNotify

Recovery:

1. This alarm may occur during initial installation and configuration of a server. No action is necessary at that time.
2. If this alarm occurs after successful initial installation and configuration of a server, contact [My Oracle Support \(MOS\)](#).

31110 - Database audit fault

Alarm Group:	SW
Description:	The Database service process (idbsvc) is impaired by a s/w fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbAuditFaultNotify

Recovery:

1. Alarm indicates an error occurred within the database audit system, but the system has recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31111 - Database merge audit in progress

Alarm Group:	COLL
Description:	Database Merge Audit between mate nodes in progress
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMergeAuditNotify

Recovery:

No action required.

31112 - DB replication update log transfer timed out

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

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	30
OID:	comcolDbRepUpLogTransTimeoutNotify
Recovery:	No action required. Contact My Oracle Support (MOS) if this occurs frequently.

31113 - DB replication manually disabled

Alarm Group:	REPL
Description:	DB Replication Manually Disabled
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolDbReplicationManuallyDisabledNotify
Recovery:	No action required.

31114 - DB replication over SOAP has failed

Alarm Group:	REPL
Description:	Database replication of configuration data via SOAP has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	3600
OID:	comcolDbReplicationSoapFaultNotify
Recovery:	<ol style="list-style-type: none"> 1. This alarm indicates a SOAP subsystem is unable to connect to a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity. 2. If no issues with network connectivity or the server are found and the problem persists, contact My Oracle Support (MOS).

31115 - Database service fault

Alarm Group:	SW
Description:	The Database service process (idbsvc) is impaired by a s/w fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbServiceFaultNotify

Recovery:

1. Alarm indicates an error occurred within the database disk service subsystem, but the system has recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31116 - Excessive shared memory

Alarm Group:	MEM
Description:	The amount of shared memory consumed exceeds configured thresholds.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolExcessiveSharedMemoryConsumptionNotify

Recovery:

Contact [My Oracle Support \(MOS\)](#).

31117 - Low disk free

Alarm Group:	DISK
Description:	The amount of free disk is below configured thresholds
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds: 300
OID: comcolLowDiskFreeNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact [My Oracle Support \(MOS\)](#).

31118 - Database disk store fault

Alarm Group: DISK
Description: Writing the database to disk failed
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolDbDiskStoreFaultNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact [My Oracle Support \(MOS\)](#).

31119 - Database updatelog overrun

Alarm Group: DB
Description: The Database update log was overrun increasing risk of data loss
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolDbUpdateLogOverrunNotify

Recovery:

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

31120 - Database updatelog write fault

Alarm Group:	DB
Description:	A Database change cannot be stored in the updatelog
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbUpdateLogWriteFaultNotify

Recovery:

1. This alarm indicates an error has occurred within the database update log subsystem, but the system has recovered.
2. If the alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31121 - Low disk free early warning

Alarm Group:	DISK
Description:	The amount of free disk is below configured early warning thresholds
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolLowDiskFreeEarlyWarningNotify

Recovery:

1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
2. If there are no files known to be unneeded, contact [My Oracle Support \(MOS\)](#).

31122 - Excessive shared memory early warning

Alarm Group:	MEM
Description:	The amount of shared memory consumed exceeds configured early warning thresholds
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal
Auto Clear Seconds: 300
OID: comcolExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

1. This alarm indicates that a server is close to exceeding the engineered limit for shared memory usage and the application software is at risk to fail. There is no automatic recovery or recovery steps.
2. Contact [My Oracle Support \(MOS\)](#).

31123 - Database replication audit command complete

Alarm Group: REPL
Description: ADIC found one or more errors that are not automatically fixable.
Severity: Info
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolDbRepAuditCmdCompleteNotify

Recovery:

No action required.

31124 - ADIC error

Alarm Group: REPL
Description: An ADIC detected errors
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolDbRepAuditCmdErrNotify

Recovery:

Contact [My Oracle Support \(MOS\)](#).

31125 - Database durability degraded

Alarm Group:	REPL
Description:	Database durability has dropped below configured durability level
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbDurabilityDegradedNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

31126 - Audit blocked

Alarm Group:	REPL
Description:	Site Audit Controls blocked an inter-site replication audit due to the number in progress per configuration.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolAuditBlockedNotify

Recovery:

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

31127 - DB Replication Audit Complete

Alarm Group:	REPL
Description:	DB replication audit completed
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	300
OID:	comcolDbRepAuditCompleteNotify
Recovery:	No action required.

31128 - ADIC Found Error

Alarm Group:	REPL
Description:	ADIC found one or more errors that are not automatically fixable.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbADICErrorNotify

Recovery:

1. This alarm indicates a data integrity error was found by the background database audit mechanism, and there is no automatic recovery.
2. Contact [My Oracle Support \(MOS\)](#).

31129 - ADIC Found Minor Issue

Alarm Group:	REPL
Description:	ADIC found one or more minor issues that can most likely be ignored
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	14400
OID:	comcolDbADICWarn

Recovery:

No action required.

31130 - Network health warning

Alarm Group:	NET
---------------------	-----

Description:	Network health issue detected
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolNetworkHealthWarningNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

31131 - DB Ousted Throttle Behind

Alarm Group:	DB
Description:	DB ousted throttle may be affecting processes.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolOustedThrottleWarnNotify

Recovery:

1. This alarm indicates that a process has failed to release database memory segments which is preventing new replication audits from taking place. There is no automatic recovery for this failure.
2. Run 'procshm -o' to identify involved processes.
3. Contact [My Oracle Support \(MOS\)](#).

31140 - Database perl fault

Alarm Group:	SW
Description:	Perl interface to Database is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbPerlFaultNotify

Recovery:

1. This alarm indicates an error has occurred within a Perl script, but the system has recovered.
2. If the alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31145 - Database SQL fault

Alarm Group:	SW
Description:	SQL interface to Database is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbSQLFaultNotify

Recovery:

1. This alarm indicates an error has occurred within the MySQL subsystem, but the system has recovered.
2. If this alarm occurs frequently, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31146 - DB mastership fault

Alarm Group:	SW
Description:	DB replication is impaired due to no mastering process (inetrep/inetrep).
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. Contact [My Oracle Support \(MOS\)](#).

31147 - DB upsynclog overrun

Alarm Group:	SW
Description:	UpSyncLog is not big enough for (WAN) replication.
Severity:	Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbUpSyncLogOverrunNotify

Recovery:

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

31148 - DB lock error detected

Alarm Group:	DB
Description:	The DB service process (idbsvc) has detected an IDB lock-related error caused by another process. The alarm likely indicates a DB lock-related programming error, or it could be a side effect of a process crash.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbLockErrorNotify

Recovery:

1. This alarm indicates an error occurred within the database disk service subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31200 - Process management fault

Alarm Group:	SW
Description:	The process manager (procmgr) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300

OID: comcolProcMgmtFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31201 - Process not running

Alarm Group: PROC

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcNotRunningNotify

Recovery:

1. This alarm indicates that the managed process exited unexpectedly due to a memory fault, but the process was automatically restarted.
2. Collect savelogs and contact [My Oracle Support \(MOS\)](#).

31202 - Unkillable zombie process

Alarm Group: PROC

Description: A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcZombieProcessNotify

Recovery:

1. This alarm indicates managed process exited unexpectedly and was unable to be restarted automatically.
2. Collect savelogs and contact [My Oracle Support \(MOS\)](#).

31206 - Process mgmt monitoring fault

Alarm Group:	SW
Description:	The process manager monitor (pm.watchdog) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolProcMgmtMonFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31207 - Process resource monitoring fault

Alarm Group:	SW
Description:	The process resource monitor (ProcWatch) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolProcResourceMonFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process monitoring subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31208 - IP port server fault

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

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolPortServerFaultNotify

Recovery:

1. This alarm indicates an error occurred within the port mapping subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31209 - Hostname lookup failed

Alarm Group:	SW
Description:	Unable to resolve a hostname specified in the NodeInfo table
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHostLookupFailedNotify

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

31213 - Process scheduler fault

Alarm Group:	SW
Description:	The process scheduler (ProcSched/runat) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolProcSchedulerFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31214 - Scheduled process fault

Alarm Group:	PROC
Description:	A scheduled process cannot be executed or abnormally terminated
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolScheduleProcessFaultNotify

Recovery:

1. This alarm indicates that a managed process exited unexpectedly due to a memory fault, but the system has recovered.
2. Contact [My Oracle Support \(MOS\)](#).

31215 - Process resources exceeded

Alarm Group:	SW
Description:	A process is consuming excessive system resources.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	14400
OID:	comcolProcResourcesExceededFaultNotify

Recovery:

1. This alarm indicates a process has exceeded the engineered limit for heap usage and there is a risk the application software will fail.
2. Because there is no automatic recovery for this condition, contact [My Oracle Support \(MOS\)](#).

31216 - SysMetric configuration error

Alarm Group:	SW
Description:	A SysMetric Configuration table contains invalid data

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolSysMetricConfigErrorNotify
Recovery:	<ol style="list-style-type: none"> 1. This alarm indicates a system metric is configured incorrectly. 2. Contact My Oracle Support (MOS).

31220 - HA configuration monitor fault

Alarm Group:	SW
Description:	The HA configuration monitor is impaired by a s/w fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaCfgMonitorFaultNotify
Recovery:	Contact My Oracle Support (MOS) .

31221 - HA alarm monitor fault

Alarm Group:	SW
Description:	The high availability alarm monitor is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaAlarmMonitorFaultNotify
Recovery:	Contact My Oracle Support (MOS) .

31222 - HA not configured

Alarm Group:	HA
Description:	High availability is disabled due to system configuration
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaNotConfiguredNotify
Recovery:	Contact My Oracle Support (MOS) .

31223 - HA Heartbeat transmit failure

Alarm Group:	HA
Description:	The high availability monitor failed to send heartbeat.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaHbTransmitFailureNotify
Recovery:	<ol style="list-style-type: none"> 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 Group:	HA
Description:	High availability configuration error
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaCfgErrorNotify

Recovery:

1. This alarm indicates a platform configuration error in the High Availability or VIP management subsystem.
2. Because there is no automatic recovery for this condition, contact [My Oracle Support \(MOS\)](#).

31225 - HA service start failure

Alarm Group:	HA
Description:	The required high availability resource failed to start.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0
OID:	comcolHaSvcStartFailureNotify

Recovery:

1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, contact [My Oracle Support \(MOS\)](#).

31226 - HA availability status degraded

Alarm Group:	HA
Description:	The high availability status is degraded due to raised alarms.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0
OID:	comcolHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#).

31227 - HA availability status failed

Alarm Group:	HA
Description:	The high availability status is failed due to raised alarms.
Severity:	Critical

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaAvailFailedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#).

31228 - HA standby offline

Alarm Group:	HA
Description:	High availability standby server is offline.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolHaStandbyOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues and/or Contact [My Oracle Support \(MOS\)](#).

31229 - HA score changed

Alarm Group:	HA
Description:	High availability health score changed
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaScoreChangeNotify

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

Alarm Group:	SW
Description:	The recent alarm event manager (raclerk) is impaired by a s/w fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolRecAlarmEvProcFaultNotify

Recovery:

1. This alarm indicates an error occurred within the alarm management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31231 - Platform alarm agent fault

Alarm Group:	SW
Description:	The platform alarm agent impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolPlatAlarmAgentNotify

Recovery:

1. This alarm indicates an error occurred within the alarm management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, contact [My Oracle Support \(MOS\)](#).

31232 - Late heartbeat warning

Alarm Group:	HA
Description:	High availability server has not received a message on specified path within the configured interval.
Severity:	Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaLateHeartbeatWarningNotify

Recovery:

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

31233 - HA Path Down

Alarm Group:	HA
Description:	High availability path loss of connectivity
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaPathDownNotify

Recovery:

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

31234 - Untrusted Time Upon Initialization

Alarm Group:	REPL
Description:	Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)

OID: comcolUtrustedTimeOnInitNotify

Recovery:

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

31235 - Untrusted Time After Initialization

Alarm Group: REPL

Description: After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, etc. There are often accompanying Platform alarms to guide correction. Generally, applications remain running, but time-stamped data is likely incorrect, reports may be negatively affected, some behavior may be improper, etc.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolUtrustedTimePostInitNotify

Recovery:

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

31236 - HA Link Down

Alarm Group: HA

Description: High availability TCP link is down.

Severity: Critical

Instance: Remote node being connected to plus the path identifier

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaLinkDownNotify

Recovery:

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

31240 - Measurements collection fault

Alarm Group:	SW
Description:	The measurements collector (statclerk) is impaired by a s/w fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolMeasCollectorFaultNotify

Recovery:

1. This alarm indicates that an error within the measurement subsystem has occurred, but that the system has recovered.
2. If this alarm occurs repeatedly, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31250 - RE port mapping fault

Alarm Group:	SW
Description:	The IP service port mapper (re.portmap) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolRePortMappingFaultNotify

Recovery:

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

31260 - SNMP Agent

Alarm Group:	SW
Description:	The SNMP agent (cmsnmpa) is impaired by a s/w fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds: 300
OID: eagleXgHlrRouterDbcomcolSnmpAgentNotify

Recovery:

1. This alarm indicates an error occurred within the SNMP subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, collect savelogs and contact [My Oracle Support \(MOS\)](#).

31270 - Logging output

Alarm Group: SW
Description: Logging output set to Above Normal
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolLoggingOutputNotify

Recovery:

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

31280 - HA Active to Standby transition

Alarm Group: HA
Description: HA active to standby activity transition
Severity: Info
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact [My Oracle Support \(MOS\)](#).

31281 - HA Standby to Active transition

Alarm Group: HA
Description: HA standby to active activity transition

Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolStandbyToActiveTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact [My Oracle Support \(MOS\)](#).

31282 - HA Management Fault

Alarm Group:	HA
Description:	The HA manager (cmha) is impaired by a software fault.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaMgmtFaultNotify

Recovery:

1. This alarm indicates an error occurred within the High Availability subsystem, but the system has automatically recovered.
2. If the alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

31283 - Lost Communication with server

Alarm Group:	HA
Description:	Highly available server failed to receive mate heartbeats
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolHaServerOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues and/or Contact [My Oracle Support \(MOS\)](#).

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Group:	HA
Description:	High availability remote subscriber has not received a heartbeat within the configured interval.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaRemoteHeartbeatWarningNotify

Recovery:

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

31285 - HA Node Join Recovery Entry

Alarm Group:	HA
Description:	High availability node join recovery entered
Severity:	Info
Instance:	Cluster set key of the DC outputting the event
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaSbrEntryNotify

Recovery:

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

31286 - HA Node Join Recovery Plan

Alarm Group:	HA
Description:	High availability node join recovery plan

Severity:	Info
Instance:	Names of HA Policies (as defined in HA policy configuration)
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaSbrPlanNotify

Recovery:

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

31287 - HA Node Join Recovery Complete

Alarm Group:	HA
Description:	High availability node join recovery complete
Severity:	Info
Instance:	Names of HA Policies (as defined in HA policy configuration)
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaSbrCompleteNotify

Recovery:

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

31290 - HA Process Status

Alarm Group:	HA
Description:	HA manager (cmha) status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaProcessStatusNotify

Recovery:

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

31291 - HA Election Status

Alarm Group:	HA
Description:	HA DC Election status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaElectionStatusNotify

Recovery:

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

31292 - HA Policy Status

Alarm Group:	HA
Description:	HA Policy plan status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaPolicyStatusNotify

Recovery:

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

31293 - HA Resource Link Status

Alarm Group:	HA
Description:	HA ResourceAgent Link status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaRaLinkStatusNotify

Recovery:

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

31294 - HA Resource Status

Alarm Group:	HA
Description:	HA Resource registration status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaResourceStatusNotify

Recovery:

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

31295 - HA Action Status

Alarm Group:	HA
Description:	HA Resource action status
Severity:	Info
Instance	N/A
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaActionStatusNotify

Recovery:

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

31296 - HA Monitor Status

Alarm Group:	HA
Description:	HA Monitor action status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaMonitorStatusNotify

Recovery:

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

31297 - HA Resource Agent Info

Alarm Group:	HA
Description:	HA Resource Agent Info
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaRaInfoNotify

Recovery:

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

31298 - HA Resource Agent Detail

Alarm Group:	HA
Description:	Resource Agent application detailed information
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaRaDetailNotify

Recovery:

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

31299 - HA Notification Status

Alarm Group:	HA
Description:	HA Notification status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300

OID: comcolHaNotificationNotify

Recovery:
No action required.

31300 - HA Control Status

Alarm Group: HA
Description: HA Control action status
Severity: Info
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaControlNotify

Recovery:
No action required.

31301 - HA Topology Events

Alarm Group: HA
Description: HA Topology events
Severity: Info
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDsrHaTopologyNotify

Recovery:
No action required.

32100 - Breaker Panel Feed Unavailable

Alarm Group: PLAT
Description: Breaker Panel Breaker Unavailable
Severity: Critical
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal

Auto Clear Seconds: 0 (zero)
OID: tpdBrkPnlFeedUnavailable

Recovery:

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Group: PLAT
Description: Breaker Panel Breaker Failure
Severity: Critical
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdBrkPnlBreakerFailure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

Alarm Group: PLAT
Description: Breaker Panel Monitoring Failure
Severity: Critical
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdBrkPnlMntFailure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32103 - Power Feed Unavailable

Alarm Group: PLAT
Description: Power Feed Unavailable
Severity: Critical
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdPowerFeedUnavail

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Group: PLAT
Description: Power Supply 1 Failure
Severity: Critical
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdPowerSupply1Failure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Group: PLAT
Description: Power Supply 2 Failure
Severity: Critical
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdPowerSupply2Failure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group: PLAT
Description: Power Supply 3 Failure
Severity: Critical

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply3Failure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32107 - Raid Feed Unavailable

Alarm Group:	PLAT
Description:	Raid Feed Unavailable
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRaidFeedUnavailable

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Group:	PLAT
Description:	Raid Power 1 Failure
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRaidPower1Failure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Group:	PLAT
Description:	Raid Power 2 Failure

Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRaidPower2Failure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Group:	PLAT
Description:	Raid Power 3 Failure
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRaidPower3Failure

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32111 - Device Failure

Alarm Group:	PLAT
Description:	Device Failure
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDeviceFailure

Recovery:

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32112 - Device Interface Failure

Alarm Group:	PLAT
---------------------	------

Description:	Device Interface Failure
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDeviceIfFailure

Recovery:

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32113 - Uncorrectable ECC memory error

Alarm Group:	PLAT
Description:	This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdEccUncorrectableError
Alarm ID:	TKSPLATCR14

Recovery:

Contact the hardware vendor to request hardware replacement.

32114 - SNMP get failure

Alarm Group:	PLAT
Description:	The server failed to receive SNMP information from the switch.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSNMPGetFailure
Alarm ID:	TKSPLATCR15

Recovery:

1. Verify device is active and responds to the ping command.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Group:	PLAT
Description:	This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedFailure
Alarm ID:	TKSPLATCR16

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running .
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

 - a) Reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32116 - TPD Server's Time Has Gone Backwards

Alarm Group:	PLAT
Description:	This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good.

Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPTimeGoneBackwards
Alarm ID:	TKSPLATCR17

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32117 - TPD NTP Offset Check Failure

Alarm Group:	PLAT
Description:	This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpOffsetCheckFailure
Alarm ID:	TKSPLATCR18

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.

2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

- a) To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start

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

32300 - Server fan failure

Alarm Group:	PLAT
Description:	This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdFanError
Alarm ID:	TKSPLATMA1

Recovery:

1. Run Syscheck in Verbose mode to determine which server fan assemblies is failing and replace the fan assembly.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32301 - Server internal disk error

Alarm Group:	PLAT
Description:	This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)

OID: tpdIntDiskError
Alarm ID: TKSPLATMA2

Recovery:

1. Run syscheck in verbose mode.
2. Determine the raid state of the mirrored disks, collect data:
 - a) cat /proc/mdstat
 - b) cat /etc/raidtab
3. Contact *My Oracle Support (MOS)* and provide the system health check output and collected data.

32302 - Server RAID disk error

Alarm Group: PLAT
Description: This alarm indicates that the offboard storage server had a problem with its hardware disks.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdRaidDiskError
Alarm ID: TKSPLATMA3

Recovery

Contact *My Oracle Support (MOS)*.

32303 - Server Platform error

Alarm Group: PLAT
Description: This alarm indicates an error such as a corrupt system configuration or missing files.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdPlatformError
Alarm ID: TKSPLATMA4

Recovery:

1. Run syscheck in verbose mode.

2. Determine the raid state of the mirrored disks, collect data:
 - a) cat /proc/mdstat
 - b) cat /etc/raidtab
3. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output and collected data.

32304 - Server file system error

Alarm Group:	PLAT
Description:	This alarm indicates unsuccessful writing to at least one of the server's file systems.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdFileSystemError
Alarm ID:	TKSPLATMA5

Recovery:

1. Run syscheck in verbose mode.
2. Address full file systems identified in syscheck output, and run syscheck in verbose mode.
3. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32305 - Server Platform process error

Alarm Group:	PLAT
Description:	This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPlatProcessError
Alarm ID:	TKSPLATMA6

Recovery:

1. Run syscheck in verbose mode.
2. Address full file systems identified in syscheck output, and run syscheck in verbose mode.
3. If alarm persists, contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32306 - Server RAM shortage error

Alarm Group:	PLAT
Description:	Not Implemented.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRamShortageError

Recovery

Contact [My Oracle Support \(MOS\)](#).

32307 - Server swap space shortage failure

Alarm Group:	PLAT
Description:	This alarm indicates that the server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSwapSpaceShortageError
Alarm ID:	TKSPLATMA8

Recovery:

1. Run syscheck in verbose mode.
2. Determine processes using swap.
 - a) Note: One method to determine the amount of swap being used by process is: `grep VmSwap /proc/<process id>/status`
3. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output and process swap usage.

32308 - Server provisioning network error

Alarm Group:	PLAT
---------------------	------

Description:	This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdProvNetworkError
Alarm ID:	TKSPLATMA9

Recovery:

1. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.
2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.
4. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, contact [My Oracle Support \(MOS\)](#).

32309 - Eagle Network A Error

Alarm Group:	PLAT
Description:	Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdEagleNetworkAError

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32310 - Eagle Network B Error

Alarm Group:	PLAT
---------------------	------

Description:	Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdEagleNetworkBError

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32311 - Sync Network Error

Alarm Group:	PLAT
Description:	Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSyncNetworkError

Recovery

Contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32312 - Server disk space shortage error

Alarm Group:	PLAT
Description:	This alarm indicates that one of the following conditions has occurred: <ul style="list-style-type: none"> • A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system. • More than 90% of the total number of available files have been allocated on the file system. • A file system has a different number of blocks than it had when installed.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskSpaceShortageError
Alarm ID:	TKSPLATMA13

Recovery:

1. Run syscheck in verbose mode.
2. Examine contents of identified volume in syscheck output to determine if any large files are in the file system. Delete unnecessary files, or move files off of server. Capture output from "du -sx <file system>".
3. Capture output from "df -h" and "df -i" commands.
4. Determine processes using the file system(s) that have exceeded the threshold.
5. Contact *My Oracle Support (MOS)* and provide the system health check output and provide additional file system output.

32313 - Server default route network error

Alarm Group:	PLAT
Description:	This alarm indicates that the default network route of the server is experiencing a problem.



Caution: When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDefaultRouteNetworkError

Recovery:

Run syscheck in verbose mode.

- If the syscheck output is: The default router at <IP_address> cannot be pinged, the router may be down or unreachable. Do the following:

- a) Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
- b) Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
- c) Check with the router administrator to verify that the router is configured to reply to pings on that interface.
- d) Rerun syscheck.
- e) If the alarm has not been cleared, collect the syscheck output and contact [My Oracle Support \(MOS\)](#).
 - If the syscheck output is: The default route is not on the provisioning network, collect the syscheck output and contact [My Oracle Support \(MOS\)](#).
 - If the syscheck output is: An active route cannot be found for a configured default route, collect the syscheck output and contact [My Oracle Support \(MOS\)](#).

32314 - Server temperature error

Alarm Group:	PLAT
Description:	The internal temperature within the server is unacceptably high.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerTemperatureError
Alarm ID:	TKSPLATMA15

Recovery:

1. Ensure that nothing is blocking the fan intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Run syscheck.
 - a) If the alarm has been cleared, the problem is resolved.
 - b) If the alarm has not been cleared, continue troubleshooting.
4. Replace the filter.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

5. Re-run syscheck.
 - a) If the alarm has been cleared, the problem is resolved.
 - b) If the alarm has not been cleared, continue troubleshooting.
6. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#).

32315 - Server mainboard voltage error

Alarm Group:	PLAT
Description:	This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerMainboardVoltageError
Alarm ID:	TKSPLATMA16

Recovery:

1. Run syscheck in verbose mode.
2. If alarm persists, contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32316 - Server power feed error

Alarm Group:	PLAT
Description:	This alarm indicates that one of the power feeds to the server has failed. If this alarm occurs in conjunction with any Breaker Panel alarm, there might be a problem with the breaker panel.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPowerFeedError
Alarm ID:	TKSPLATMA17

Recovery:

1. Verify that all the server power feed cables to the server that is reporting the error are securely connected.
2. Check to see if the alarm has cleared

- If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, continue with the next step.
3. Follow the power feed to its connection on the power source. Ensure that the power source is ON and that the power feed is properly secured.
 4. Check to see if the alarm has cleared
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, continue with the next step.
 5. If the power source is functioning properly and the wires are all secure, have an electrician check the voltage on the power feed.
 6. Check to see if the alarm has cleared
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, continue with the next step.
 7. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#).

32317 - Server disk health test error

Alarm Group:	PLAT
Description:	Either the hard drive has failed or failure is imminent.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskHealthError
Alarm ID:	TKSPLATMA18

Recovery:

1. Run syscheck in verbose mode.
2. Replace the hard drives that have failed or are failing.
3. Re-run syscheck in verbose mode.
4. Perform the recovery procedures for the other alarms that may accompany this alarm.
5. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#) and provide the system health check output. .

32318 - Server disk unavailable error

Alarm Group:	PLAT
Description:	The smartd service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskUnavailableError
Alarm ID:	TKSPLATMA19

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32319 - Device error

Alarm Group:	PLAT
Description:	This alarm indicates that the offboard storage server had a problem with its disk volume filling up.
Severity:	Major
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDeviceError
Alarm ID:	TKSPLATMA20

Recovery

Contact the [My Oracle Support \(MOS\)](#).

32320 - Device interface error

Alarm Group:	PLAT
Description:	This alarm indicates that the IP bond is either not configured or down.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDeviceIfError
Alarm ID:	TKSPLATMA21

Recovery:

1. Run syscheck in verbose mode.
2. Investigate the failed bond, and slave devices, configuration:
 1. Navigate to /etc/sysconfig/network-scripts for the persistent configuration of a device.
3. Determine if the failed bond, and slave devices, has been administratively shut down or has operational issues:
 1. cat /proc/net/bonding/bondX, where X is bond designation
 2. ethtool <slave device>
4. If bond, and slaves, are healthy attempt to administratively bring bond up:
 1. ifup bondX
5. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#) and provide the system health check output and the output of the above investigation.

32321 - Correctable ECC memory error

Alarm Group:	PLAT
Description:	This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdEccCorrectableError
Alarm ID:	TKSPLATMA22

Recovery:

1. No recovery necessary.
2. If the condition persists, verify the server firmware. Update the firmware if necessary, and re-run syscheck in verbose mode. Otherwise if the condition persists and the firmware is up to date, contact the hardware vendor to request hardware replacement.

32322 - Power Supply A error

Alarm Group:	PLAT
Description:	This alarm indicates that power supply 1 (feed A) has failed.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply1Error
Alarm ID:	TKSPLATMA23

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. Run syscheck in verbose mode. The output will provide details about what is wrong with the power supply.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#) and provide them the syscheck verbose output. Power supply 1 (feed A) will probably need to be replaced.

32323 - Power Supply B error

Alarm Group:	PLAT
Description:	This alarm indicates that power supply 2 (feed B) has failed.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply2Error
Alarm ID:	TKSPLATMA24

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. Run syscheck in verbose mode. The output will provide details about what is wrong with the power supply.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#) and provide them the syscheck verbose output. Power supply 2 (feed B) will probably need to be replaced.

32324 - Breaker panel feed error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not receiving information from the breaker panel relays.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdBrkPnlFeedError

Alarm ID: TKSPLATMA25

Recovery:

1. Verify that the same alarm is displayed by multiple servers:
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.
3. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#) to request that the breaker panel be replaced.

32325 - Breaker panel breaker error

Alarm Group: PLAT

Description: This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see [Figure 4: 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.

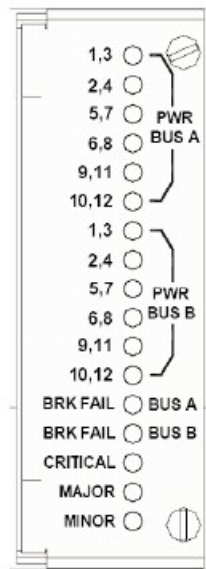


Figure 4: Breaker Panel LEDs

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	TPDBrkPnlBreakerError
Alarm ID:	TKSPLATMA26

Recovery:

1. Verify that the same alarm is displayed by both servers. The single breaker panel normally sends alarm information to both servers:
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by both servers, go to the next step.
2. For each breaker assignment, verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green .

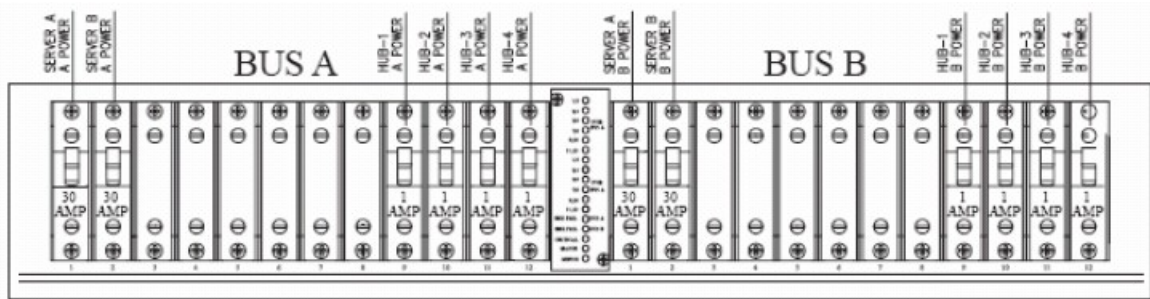


Figure 5: Breaker Panel Setting

If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Perform the following steps to correct this problem:

- Verify that the customer provided source for the affected power feed is operational. If the power source is properly functioning, have an electrician remove the plastic cover from the rear of the breaker panel and verify the power source is indeed connected to the input power feed connector on the rear of the breaker panel. Correct any issues found.
- Check the LEDs in the PWR BUS A group and the PWR BUS B group again.
 1. If the LEDs are now illuminated Green, the issue has been resolved. Proceed to step 4 to verify that the alarm has been cleared.
 2. If the LEDs are still illuminated Red, continue to the next sub-step.
- Have the electrician verify the integrity of the input power feed. The input voltage should measure nominally -48VDC (that is, between -41VDC and -60VDC). If the supplied voltage is not within the acceptable range, the input power source must be repaired or replaced.

Note:

Be sure the voltmeter is connected properly. The locations of the BAT and RTN connections are in mirror image on either side of the breaker panel.

If the measured voltage is within the acceptable range, the breaker panel may be malfunctioning. The breaker panel must be replaced.

- Check the LEDs in the PWR BUS A group and the PWR BUS B group again after the necessary actions have been taken to correct any issues found
 1. If the LEDs are now illuminated Green, the issue has been resolved and proceed to step 4 to verify that the alarm has been cleared.
 2. If the LEDs are still illuminated Red, skip to step 5
- 3. Check the BRK FAIL LEDs for BUS A and for BUS B.
 - If one of the BRK FAIL LEDs is illuminated Red, then one or more of the respective Input Breakers has tripped. (A tripped breaker is indicated by the toggle located in the center position.) Perform the following steps to repair this issue:
 - a) For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.
 - b) After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, run syscheck and contact [My Oracle Support \(MOS\)](#)

4. If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise run syscheck and contact [My Oracle Support \(MOS\)](#)
5. Run syscheck.
 - If the alarm has been cleared, the problem is resolved.
 - If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#)

32326 - Breaker panel monitoring error

Alarm Group:	PLAT
Description:	This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself. Note: When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm: <ul style="list-style-type: none"> • 32324 – Breaker panel feed error • 32325 – Breaker panel breaker error until the Breaker Panel Monitoring Error has been corrected.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdBrkPnlMntError
Alarm ID:	TKSPLATMA27

Recovery:

1. Verify that the same alarm is displayed by both servers (the single breaker panel normally sends alarm information to both servers):
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by both servers, go to the next step.
2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).

3. Run syscheck..
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, contact [My Oracle Support \(MOS\)](#)

32327 - Server HA Keepalive error

Alarm Group:	PLAT
Description:	This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaKeepaliveError
Alarm ID:	TKSPLATMA28

Recovery:

1. Determine if the mate server is currently down and bring it up if possible.
2. Determine if the keepalive interface is down.
3. Determine if heartbeat is running (service TKLCha status).
 - Note:** This step may require command line ability.
4. Contact [My Oracle Support \(MOS\)](#).

32328 - DRBD is unavailable

Alarm Group:	PLAT
Description:	This alarm indicates that DRBD is not functioning properly on the local server. The DRBD state (disk state, node state, and/or connection state) indicates a problem.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdUnavailable
Alarm ID:	TKSPLATMA29

Recovery

Contact [My Oracle Support \(MOS\)](#).

32329 - DRBD is not replicating

Alarm Group:	PLAT
Description:	This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdNotReplicating
Alarm ID:	TKSPLATMA30

Recovery

Contact [My Oracle Support \(MOS\)](#).

32330 - DRBD peer problem

Alarm Group:	PLAT
Description:	This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdPeerProblem
Alarm ID:	TKSPLATMA31

Recovery

Contact the [My Oracle Support \(MOS\)](#).

32331 - HP disk problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with either a physical or logical disk in the HP disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskProblem
Alarm ID:	TKSPLATMA32

Recovery:

1. Run syscheck in verbose mode.
2. If "Cache Status" is OK and "Cache Status Details" reports a cache error was detected so diagnostics should be run, there probably is no battery and data was left over in the write cache not getting flushed to disk and won't since there is no battery.
3. If "Cache Status" is "Permanently Disabled" and "Cache Status Details" indicated the cache is disabled, if there is no battery then the firmware should be upgraded.
4. Re-run syscheck in verbose mode if firmware upgrade was necessary.
5. If condition persists, contact [My Oracle Support \(MOS\)](#) and provide the system health check output. The disk may need to be replaced.

32332 - HP Smart Array controller problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskCtrlrProblem
Alarm ID:	TKSPLATMA33

Recovery:

1. Run syscheck in verbose mode.
2. If condition persists, contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32333 - HP hpacucliStatus utility problem

Alarm Group:	PLAT
---------------------	------

Description:	This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus/hpDiskStatus daemon is either not running, or hung.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHPACUCLIProblem
Alarm ID:	TKSPLATMA34

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the HP disk status daemon is running. If not running verify that it was not administratively stopped.

Note: The disk status daemon is named either TKLChpacucli or TPDhpDiskStatus in more recent versions of TPD.

- a) Executing "status TPDhpDiskStatus", or "status TKLChpacucli" depending on TPD release, should produce output indicating that the process is running.
4. If not running, attempt to start the HP disk status process : "start TPDhpDiskStatus", or if appropriate "start TKLChpacucli" .
 5. Verify that there are no hpssacli, or hpacucli, error messages in /var/log/messages. If there are this could indicate that the HP utility is hung. If the HP hpssacli utility, or hpacucli utility, is hung, proceed with next step.
 6. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output, and savelogs_plat output.

32334 - Multipath device access link problem

Alarm Group:	PLAT
Description:	One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdMpathDeviceProblem

Recovery:

Contact [My Oracle Support \(MOS\)](#).

32335 - Switch link down error

Alarm Group:	PLAT
Description:	The link is down.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSwitchLinkDownError
Alarm ID:	TKSPLATMA36

Recovery:

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#) to determine who should verify port settings on both the server and the switch.

32336 - Half Open Socket Limit

Alarm Group:	PLAT
Description:	This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHalfOpenSockLimit
Alarm ID:	TKSPLATMA37

Recovery:

1. Run syscheck in verbose mode.
2. Determine what process and address reports a state of SYN_RECV and collect data:
 - netstat -nap.
3. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output and collected data.

32337 - E5-APP-B Firmware Flash

Alarm Group:	PLAT
Description:	This alarm indicates that there was an error while trying to update the firmware flash on the E5-APP-B cards.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdFlashProgramFailure
Alarm ID:	TKSPLATMA38

Recovery

Contact [My Oracle Support \(MOS\)](#).

32338 - E5-APP-B Serial mezzanine seating

Alarm Group:	PLAT
Description:	This alarm indicates that a connection to the serial mezzanine board may not be properly seated.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSerialMezzUnseated
Alarm ID:	TKSPLATMA39

Recovery

1. Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.
2. It is recommended to contact [My Oracle Support \(MOS\)](#) if reseating the cables does not clear the alarm.

32339 - TPD Max Number Of Running Processes Error

Alarm Group:	PLAT
Description:	This alarm indicates that the maximum number of running processes has reached the major threshold.
Severity:	Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdMaxPidLimit
Alarm ID:	TKSPLATMA40

Recovery:

1. Run syscheck in verbose mode.
2. Execute 'pstree' to see what pids are on the system and what process created them. Collect the output of command, and review the output to determine the process responsible for the alarm.
3. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output, and pid output.

32340 - TPD NTP Daemon Not Synchronized Error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedError
Alarm ID:	TKSPLATMA41

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

 - a) To reset date:

- sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32341 - TPD NTP Daemon Not Synchronized Error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNeverSynchronized
Alarm ID:	TKSPLATMA42

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

 - a) To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32342 - NTP Offset Check Error

Alarm Group:	PLAT
---------------------	------

Description:	This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpOffsetCheckError
Alarm ID:	TKSPLATMA43

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.

2. If ntp peer is reachable, restart the ntpd service.

3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

- a) To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start

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

32343 - TPD RAID disk

Alarm Group:	PLAT
Description:	This alarms indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskProblem

Alarm ID: TKSPLATMA44

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32344 - TPD RAID controller problem

Alarm Group: PLAT

Description: This alarms indicates that RAID controller needs intervention.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskCtrlrProblem

Alarm ID: TKSPLATMA45

Recovery:

1. Run syscheck in verbose mode.
2. Verify firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32345 - Server Upgrade snapshot(s) invalid

Alarm Group: PLAT

Description: This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdUpgradeSnapshotInvalid

Alarm ID: TKSPLATMA46

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. If alarm persists, contact [My Oracle Support \(MOS\)](#).

32346 - OEM hardware management service reports an error

Alarm Group:	PLAT
Description:	This alarms indicates that OEM hardware management service reports an error.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdOEMHardware
Alarm ID:	TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32347 - The hwmgmtcliStatus daemon needs intervention

Alarm Group:	PLAT
Description:	This alarms indicates the hwmgmtcliStatus daemon is not running or is not responding.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHWMGMTCLIPProblem
Alarm ID:	TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the hwmgmt process is running. If not running verify that it was not administratively stopped.
 - Executing "service hwmgmt status" should produce output indicating that the process is running.
 - If not running attempt to start process "service hwmgmt status".
4. Determine if the TKLChwmgmtcli process is running. If not running verify that it was not administratively stopped.

- Executing "status TKLChwmgmtcli" should produce output indicating that the process is running.
 - If not running attempt to start process "start TKLChwmgmtcli".
5. Verify that there are no hwmgmt error messages in /var/log/messages. If there are this could indicate that the Oracle utility is hung. If hwmgmt process is hung, proceed with next step.
 6. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32348 - The FIPS subsystem needs intervention

Alarm Group:	PLAT
Description:	This alarm indicates the FIPS subsystem is not running or has encountered errors.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdFipsSubsystemProblem

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32349 - HIDS has detected file tampering

Alarm Group:	PLAT
Description:	This alarm indicates HIDS has detected file tampering.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHidsFileTampering

Recovery:

Contact [My Oracle Support \(MOS\)](#).

32350 - Security Process Terminated

Alarm Group:	PLAT
---------------------	------

Description:	This alarm indicates that the security process monitor is not running.
Severity:	Major
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSecurityProcessDown
Recovery:	Contact My Oracle Support (MOS) .

32500 - Server disk space shortage warning

Alarm Group:	PLAT
Description:	This alarm indicates that one of the following conditions has occurred: <ul style="list-style-type: none"> • A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system. • More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskSpaceShortageWarning
Alarm ID:	TKSPLATMI1
Recovery:	<ol style="list-style-type: none"> 1. Run syscheck in verbose mode. 2. Examine contents of identified volume in syscheck output to determine if any large files are in the file system. Delete unnecessary files, or move files off of server. Capture output from "du -sx <file system>". 3. Capture output from "df -h" and "df -i" commands. 4. Determine processes using the file system(s) that have exceeded the threshold. 5. Contact My Oracle Support (MOS), provide the system health check output, and provide additional file system output.

32501 - Server application process error

Alarm Group:	PLAT
---------------------	------

Description:	This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdApplicationProcessError
Alarm ID:	TKSPLATMI2

Recovery:

1. Run syscheck in verbose mode.
2. If the alarm has been cleared, then the problem is solved.
3. If the alarm has not been cleared, determine the run level of the system.
 - If system run level is not 4, determine why the system is operating at that run level.
 - If system run level is 4, determine why the required number of instances processes are not running.
4. For additional assistance, contact [My Oracle Support \(MOS\)](#) and provide the syscheck output.

32502 - Server hardware configuration error

Alarm Group:	PLAT
Description:	This alarm indicates that one or more of the server's hardware components are not in compliance with specifications (refer to the appropriate hardware manual).
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHardwareConfigError
Alarm ID:	TKSPLATMI3

Recovery:

1. Run syscheck in verbose mode.
2. Contact the hardware vendor to request a hardware replacement.

32503 - Server RAM shortage warning

Alarm Group:	PLAT
---------------------	------

Description:	This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRamShortageWarning
Alarm ID:	TKSPLATMI4

Recovery

1. Refer to MPS-specific documentation for information regarding this alarm.
2. Contact the [My Oracle Support \(MOS\)](#).

32504 - Software Configuration Error

Alarm Group:	PLAT
Description:	This alarm is generated by the MPS syscheck software package and is not part of the PLAT distribution.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSoftwareConfigError

Recovery

Contact [My Oracle Support \(MOS\)](#).

32505 - Server swap space shortage warning

Alarm Group:	PLAT
Description:	This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time. Note: For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.
Severity:	Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSwapSpaceShortageWarning
Alarm ID:	TKSPLATMI6

Recovery:

1. Run syscheck in verbose mode.
2. Determine which processes are using swap.
 - a) List application processes and determine the process id.
 - b) Determine how much swap each process is using. One method to determine the amount of swap being used by process is:
 - `grep VmSwap /proc/<process id>/status`
3. Contact [My Oracle Support \(MOS\)](#), provide the system health check output, and process swap usage.

32506 - Server default router not defined

Alarm Group:	PLAT
Description:	This alarm indicates that the default network route is either not configured or the current configuration contains an invalid IP address or hostname.



Caution: When changing the server's network routing configuration it is important to verify that the modifications will not impact the method of connectivity for the current login session. It is also crucial that this information not be entered incorrectly or set to improper values. Incorrectly modifying the server's routing configuration may result in total loss of remote network access.

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDefaultRouteNotDefined
Alarm ID:	TKSPLATMI7

Recovery:

1. Run syscheck in verbose mode.
2. If the syscheck output is: The default router at <IP_address> cannot be pinged, the router may be down or unreachable. Do the following:

- a) Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
 - b) Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
 - c) Check with the router administrator to verify that the router is configured to reply to pings on that interface.
 - d) Rerun syscheck.
3. If the alarm has not cleared, collect the syscheck output and contact [My Oracle Support \(MOS\)](#).

32507 - Server temperature warning

Alarm Group:	PLAT
Description:	This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerTemperatureWarning
Alarm ID:	TKSPLATMI8

Recovery:

1. Ensure that nothing is blocking the fan intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Run syscheck.
4. Replace the filter (refer to the appropriate hardware manual).

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the filter is replaced before the alarm cleared.

5. Run syscheck.
6. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#).

32508 - Server core file detected

Alarm Group:	PLAT
---------------------	------

Description:	This alarm indicates that an application process has failed and debug information is available.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerCoreFileDetected
Alarm ID:	TKSPLATMI9

Recovery:

1. Contact [My Oracle Support \(MOS\)](#) to create a service request.
2. On the affected server, execute this command:

```
ll /var/TKLC/core
```

Add the command output to the service request. Include the date of creation found in the command output.

3. Attach core files to the [My Oracle Support \(MOS\)](#) service request.
4. The user can remove the files to clear the alarm with this command:

```
rm -f /var/TKLC/core/<coreFileName>
```

32509 - Server NTP Daemon not synchronized

Alarm Group:	PLAT
Description:	This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedWarning
Alarm ID:	TKSPLATMI10

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.

- c) Verify the ntp peer configuration; execute `ntpq -p` and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute `ntpstat` to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
 3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

 - a) To reset date:
 - `sudo service ntpd stop`
 - `sudo ntpdate <ntp server ip>`
 - `sudo service ntpd start`
 4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32510 - CMOS battery voltage low

Alarm Group:	PLAT
Description:	The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdCMOSBatteryVoltageLow
Alarm ID:	TKSPLATMI11
Recovery:	Contact My Oracle Support (MOS) .

32511 - Server disk self test warning

Alarm Group:	PLAT
Description:	A non-fatal disk issue (such as a sector cannot be read) exists.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds: 0 (zero)
OID: tpdSmartTestWarn
Alarm ID: TKSPLATMI12

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#).

32512 - Device warning

Alarm Group: PLAT
Description: This alarm indicates that either we are unable to perform an `snmpget` command on the configured SNMP OID or the value returned failed the specified comparison operation.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdDeviceWarn
Alarm ID: TKSPLATMI13

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#).

32513 - Device interface warning

Alarm Group: PLAT
Description: This alarm can be generated by either an SNMP trap or an IP bond error.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdDeviceIfWarn
Alarm ID: TKSPLATMI14

Recovery:

1. Run syscheck in verbose mode.

2. Contact [My Oracle Support \(MOS\)](#).

32514 - Server reboot watchdog initiated

Alarm Group:	PLAT
Description:	This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdWatchdogReboot
Alarm ID:	TKSPLATMI15
Recovery:	Contact My Oracle Support (MOS) .

32515 - Server HA failover inhibited

Alarm Group:	PLAT
Description:	This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaInhibited
Alarm ID:	TKSPLATMI16
Recovery:	Contact My Oracle Support (MOS) .

32516 - Server HA Active to Standby transition

Alarm Group:	PLAT
Description:	This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaActiveToStandbyTrans
Alarm ID:	TKSPLATMI17
Recovery:	Contact My Oracle Support (MOS) .

32517 - Server HA Standby to Active transition

Alarm Group:	PLAT
Description:	This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaStandbyToActiveTrans
Alarm ID:	TKSPLATMI18
Recovery:	Contact My Oracle Support (MOS) .

32518 - Platform Health Check failure

Alarm Group:	PLAT
Description:	This alarm is used to indicate a configuration error.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHealthCheckFailed
Alarm ID:	TKSPLATMI19
Recovery:	

Contact [My Oracle Support \(MOS\)](#).

32519 - NTP Offset Check failure

Alarm Group:	PLAT
Description:	This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the NTP server and the offset limit that the application has set for the system.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpOffsetCheckWarning
Alarm ID:	TKSPLATMI20

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

- a) To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32520 - NTP Stratum Check failure

Alarm Group:	PLAT
Description:	This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm

message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpStratumCheckFailed
Alarm ID:	TKSPLATMI21

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

 - a) To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32521 - SAS Presence Sensor Missing

Alarm Group:	PLAT
Description:	This alarm indicates that the T1200 server drive sensor is not working.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	sasPresenceSensorMissing

Alarm ID: TKSPLATMI22

Recovery:
Contact [My Oracle Support \(MOS\)](#).

32522 - SAS Drive Missing

Alarm Group: PLAT

Description: This alarm indicates that the number of drives configured for this server is not being detected.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: sasDriveMissing

Alarm ID: TKSPLATMI23

Contact [My Oracle Support \(MOS\)](#).

32523 - DRBD failover busy

Alarm Group: PLAT

Description: This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdFailoverBusy

Alarm ID: TKSPLATMI24

Recovery

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 the [My Oracle Support \(MOS\)](#).

32524 - HP disk resync

Alarm Group: PLAT

Description:	This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskResync
Alarm ID:	TKSPLATMI25
Recovery:	<ol style="list-style-type: none"> 1. Run syscheck in verbose mode. 2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck. 3. If the alarm persists, contact My Oracle Support (MOS) and provide the syscheck output.

32525 - Telco Fan Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected an issue with an internal fan.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoFanWarning
Alarm ID:	TKSPLATMI26
Recovery:	<p>Contact the vendor to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.</p> <p>Note: My Oracle Support (MOS) personnel can perform an <code>snmpget</code> command or log into the switch to get detailed fan status information.</p>

32526 - Telco Temperature Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoTemperatureWarning
Alarm ID:	TKSPLATMI27

Recovery:

1. Lower the ambient air temperature around the switch as low as possible.
2. If problem persists, contact [My Oracle Support \(MOS\)](#).

32527 - Telco Power Supply Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoPowerSupplyWarning
Alarm ID:	TKSPLATMI28

Recovery:

1. Verify the breaker was not tripped.
2. If 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 Group:	PLAT
---------------------	------

Description:	This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdInvalidBiosValue
Alarm ID:	TKSPLATMI29
Recovery:	Change the BIOS values to the expected values which involves re-booting the server. Contact My Oracle Support (MOS) for directions on changing the BIOS.

32529 - Server Kernel Dump File Detected

Alarm Group:	PLAT
Description:	This alarm indicates that the kernel has crashed and debug information is available.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerKernelDumpFileDetected
Alarm ID:	TKSPLATMI30
Recovery:	<ol style="list-style-type: none"> 1. Run syscheck in verbose mode. 2. Contact My Oracle Support (MOS).

32530 - TPD Upgrade Failed

Alarm Group:	PLAT
Description:	This alarm indicates that a TPD upgrade has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds: 0 (zero)
OID: pdServerUpgradeFailed
Alarm ID: TKSPLATMI31
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32531 - Half Open Socket Warning Limit

Alarm Group: PLAT
Description: This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdHalfOpenSocketWarning
Alarm ID: TKSPLATMI32
Recovery:
 1. Run syscheck in verbose mode.
 2. Contact [My Oracle Support \(MOS\)](#).

32532 - Server Upgrade Pending Accept/Reject

Alarm Group: PLAT
Description: This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdServerUpgradePendingAccept
Alarm ID: TKSPLATMI33
Recovery:
 Follow the steps in the application procedure to accept or reject the upgrade.

32533 - TPD Max Number Of Running Processes Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the maximum number of running processes has reached the minor threshold.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdMaxPidWarning
Alarm ID:	TKSPLATMI34

Recovery:

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#).

32534 - TPD NTP Source Is Bad Warning

Alarm Group:	PLAT
Description:	This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPSourceIsBad
Alarm ID:	TKSPLATMI35

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a) Ensure ntpd service is running.
 - b) Verify the content of the /etc/ntp.conf file is correct for the server.
 - c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

a) To reset date:

- sudo service ntpd stop
- sudo ntpdate <ntp server ip>
- sudo service ntpd start

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

32535 - TPD RAID disk resync

Alarm Group:	PLAT
Description:	This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskResync
Alarm ID:	TKSPLATMI36
Recovery:	<ol style="list-style-type: none"> 1. Run syscheck in verbose mode. 2. If this alarm persists for several hours (depending on a load of a server, rebuilding an array can take multiple hours to finish), contact My Oracle Support (MOS).

32536 - TPD Server Upgrade snapshot(s) warning

Alarm Group:	PLAT
Description:	This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds: 0 (zero)
OID: tpdUpgradeSnapshotWarning
Alarm ID: TKSPLATMI37

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. Contact [My Oracle Support \(MOS\)](#)

32537 - FIPS subsystem warning event

Alarm Type: PLAT
Description: This alarm indicates that the FIPS subsystem requires a reboot in order to complete configuration.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdFipsSubsystemWarning

Recovery

If alarm doesn't clear on its own, contact [My Oracle Support \(MOS\)](#).

32700 - Telco Switch Notification

Alarm Group: PLAT
Description: Telco Switch Notification
Severity: Info
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Throttle Seconds: 86400
OID: tpdTelcoSwitchNotification

Recovery:

Contact [My Oracle Support \(MOS\)](#).

32701 - HIDS Initialized

Alarm Group: PLAT
Description: This alarm indicates HIDS was initialized.

Severity	Info
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID	tpdHidsBaselineCreated
Recovery:	
	Contact My Oracle Support (MOS) .

32702 - HIDS Baseline Deleted

Alarm Group:	PLAT
Description:	HIDS baseline was deleted.
Severity:	Info
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID:	tpdHidsBaselineDeleted
Recovery:	
	Contact My Oracle Support (MOS) .

32703 - HIDS Enabled

Alarm Group:	PLAT
Description:	HIDS was enabled.
Severity:	Info
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID:	tpdHidsEnabled
Recovery:	
	Contact My Oracle Support (MOS) .

32704 - HIDS Disabled

Alarm Group:	PLAT
Description:	HIDS was disabled.
Severity:	Info

Instance N/A
HA Score Normal
Auto Clear Seconds N/A
OID: tpdHidsDisabled
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32705 - HIDS Monitoring Suspended

Alarm Group: PLAT
Description: HIDS monitoring suspended.
Severity: Info
Instance N/A
HA Score Normal
Auto Clear Seconds N/A
OID: tpdHidsSuspended
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32706 - HIDS Monitoring Resumed

Alarm Group: PLAT
Description: HIDS monitoring resumed.
Severity: Info
Instance N/A
HA Score Normal
Auto Clear Seconds N/A
OID: tpdHidsResumed
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32707 - HIDS Baseline Updated

Alarm Group: PLAT
Description: HIDS baseline updated.
Severity: Info
Instance N/A

HA Score	Normal
Auto Clear Seconds	N/A
OID:	tpdHidsBaselineUpdated
Recovery:	
Contact My Oracle Support (MOS) .	

Key Performance Indicators (KPIs)

Topics:

- [General KPIs information.....257](#)
- [EXHR KPIs.....259](#)
- [PDBI KPIs.....260](#)
- [SS7/Sigtran KPIs.....261](#)
- [Throttling KPIs.....261](#)

This section provides general information about KPIs and lists the KPIs that can appear on the **Status & Manage > KPIs** GUI page.

General KPIs information

This section provides general information about KPIs, the **Status and Manage > KPI** page, and how to view KPIs.

KPIs overview

Key Performance Indicators (KPIs) allow you to monitor system performance data, including CPU, memory, swap space, and uptime per server. This performance data is collected from all servers within the defined topology.

The KPI display function resides on all OAM servers. Servers that provide a GUI connection rely on KPI information merged to that server. The Network OAMP servers maintain status information for all servers in the topology. System OAM servers have reliable information only for servers within the same network element.

The Status and Manage KPIs page displays performance data for the entire system. KPI data for the entire system is updated every 60 seconds. If data is not currently being collected for a particular server, the KPI for that server will be shown as N/A.

KPIs

The **Status & Manage > KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAM server or an SOAM server.

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 NOAM server or an SOAM server. Collection of KPI data is handled solely by NOAM servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the **KPIs > Export** page.

Table 12: Schedule KPI Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting KPIs

You can schedule periodic exports of security log data from the **KPIs** page. KPI data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **KPIs** page, only filtered data is exported.

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

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 **KPIs [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 for frequencies other than **Daily** or **Weekly**.
8. Select the **Day of Week**.
Note: **Day of Week** is not an option for frequencies other **Weekly**.
9. Click **OK** 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](#)

EXHR KPIs

Table 13: EXHR KPIs

Measurement Tag	Description
ExhrGttExceptionRoutingtg	The total number of messages that were Exception Routed
ExhrGttPerformed	The total number of global title translations performed
ExhrMlrPerformed	Total number of messages that were MLR Performed. IMSI/DN found in MAP Layer and in Database plus the message was successfully routed

PDBI KPIs

Table 14: PDBI KPIs

Measurement Tag	Description
PdbiConnections	The number of PDBI client connections currently established. A single connection includes a client having successfully established a TCP/IP connection, sent a PDBI connect message, and having received a successful response.
PdbiMsgsDiscarded	The number of PDBI messages discarded per second. PDBI messages being discarded is due to the connection being shutdown, server being shutdown, server's role switching from active to standby, or transaction not becoming durable within the allowed amount of time.
PdbiMsgsFailed	The number of PDBI messages that have failed to be processed due to errors per second.
PdbiMsgsImported	The number of PDBI messages imported per second.
PdbiMsgsReceived	The number of PDBI messages that have been received per second.
PdbiMsgsSent	The number of PDBI messages sent per second.
PdbiMsgsSuccessful	The number of PDBI messages that have been successfully processed per second.
PdbiTxnAborted	The number of PDBI transactions aborted per second.
pdbiTxnActive	The number of PDBI transactions that are currently active (Normal transaction mode only).
PdbiTxnCommitted	The number of PDBI transactions that have been successfully committed per second to the database (memory and on disk) on the active server of the primary NOAM cluster.
PdbiTxnFailed	The number of PDBI transactions that have failed to be started, committed, or aborted due to errors per second.
PdbiTxnNonDurable	The number of transactions that have been committed, but are not yet durable. Responses for the associated requests are not sent until the transaction has become durable.

SS7/Sigtran KPIs

Table 15: SS7/Sigtran KPIs

Variable	Description
SCCP Recv Msgs/Sec	SCCP messages received per second.
SCCP Xmit Msgs/Sec	SCCP messages transmitted per second.
SS7 Process CPU Utilization	The average percent of SS7 Process CPU utilization on an MP server.
Ingress Message Rate	The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue.
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent.
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received.

Throttling KPIs

Table 16: Throttling KPIs

KPI Column Name	KPI Description
ThrottleAllow	The number of times a message was allowed, per second
ThrottleDiscard	The number of messages that were discarded as a result of matching a rule, per second
ThrottleDiscardTCAP	The number of times a TCAP error was returned in conjunction with a discard, per second
ThrottleDiscardUDTS	The number of times a UDTS was returned in conjunction with a discard, per second
ThrottleMatch	The number of messages that matched a rule, per second
ThrottleSimulation	The number of times a message matched a rule in the 'Simulation' mode but was not acted upon, per second
ThrottleWhitelistHit	The number of times a message matched a rule with Whitelist enabled, and the subscriber was in the Dn/Imsi Whitelist, per second

Key Performance Indicators (KPIs)

KPI Column Name	KPI Description
ThrottleWhitelistMiss	The number of times a message matched a rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist, per second

Chapter 5

Measurements

Topics:

- *General measurements information.....264*
- *Communication Agent (ComAgent) Exception measurements.....268*
- *Communication Agent (ComAgent) Performance measurements.....298*
- *HLR Measurements.....317*
- *OAM measurements.....322*
- *SS7/Sigtran Measurements.....324*
- *Throttling measurements.....404*
- *Transport Exception measurements.....409*
- *Transport Usage measurements.....417*
- *Transport Performance measurements.....420*

This section provides general information about measurements (including measurement procedures), and lists the measurements that display on measurement reports.

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 (NOAM, 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 17: Measurements Elements

Element	Description	Data Input Notes
Scope	Network Elements, Server Groups, Resource Domains, Places and Place Associations for which the measurements report can be run. Note: Measurements for SOAM network elements are not available in systems that do not support SOAMs.	Format: Pulldown list 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 Note: If no selection is made, the default scope is Entire Network. Default: Entire Network
Report	A selection of reports	Format: Pulldown list Range: Varies depending on application Default: Group
Column Filter	The characteristics for filtering the column display	Format: Pulldown list Range: Sub-measurement Sub-measurement Ranges: <ul style="list-style-type: none"> • Like: A pattern-matching distinction for sub-measurement name, for example, 123* matches any sub-measurement that begins with 123. • 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
Time Range	The interval of time for which the data is being reported, beginning or ending on a specified date.	Format: Pulldown list Range: Days, Hours, Minutes, Seconds Interval Reference Point: Ending, Beginning Default: Days

Generating a measurements report

Use this procedure to generate and view a measurements report.

1. Select **Measurements > Report**.

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.

Measurements data export elements

This table describes the elements on the **Measurements > Report [Export]** page.

Table 18: Schedule Measurement Data Export Elements

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

Element	Description	Data Input Notes
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting 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 and 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](#).

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](#)

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 19: Communication Agent Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
CADDataFIFOQueueFul	StackEvents discarded due to ComAgent DataFIFO queue full condition.	30 min
CADSTxDscrdCong	Number of egress stack events discarded because the congestion level of the connection exceeded the stack events' priority level.	30 min
CAHSRsrcErr	Number of times that ComAgent receives in a heartbeat stack event status concerning a known Resource but an unknown Sub-Resource.	30 min
CAHSTxDscrdCongSR	Number of stack events discarded due to HA Service Sub-Resource congestion.	30 min
CAHSTxDscrdIntErrSR	Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.	30 min
CAHSTxDscrdUnavailSR	Number of stack events discarded because they were submitted to an Unavailable Sub-Resource of a given Resource.	30 min

Measurement Tag	Description	Collection Interval
CAHSTxDscrdUnknownSR	Number of egress stack events discarded because they referred to a known Resource and an unknown Sub-Resource.	30 min
CAHSTxDscrdUnkwnRsrc	Number of egress stack events discarded because they referred to an unknown Resource.	30 min
CAHSTxRsrc	Number of egress stack events that were routed to a known Resource.	30 min
CAMx FIFOQueueFul	StackEvents discarded due to ComAgent Mx FIFO queue full condition.	30 min
CAPSTxDscrdCongPeer	Number of egress events discarded because Peer congestion.	30 min
CAPSTxDscrdUnavailGrp	Number of egress stack events discarded because they referred to a Peer Group which was unavailable.	30 min
CAPSTxDscrdUnkwnGrp	Number of egress stack events discarded because they referred to a Peer Group which was unknown.	30 min
CARsrcPoolFul	ComAgent internal resource pool exhaustion condition	30 min
CARSTxDscrdCong	Number of stack events discarded due to Routed Service congestion.	30 min
CARSTxDscrdSvcUnavail	Number of stack events discarded because they were submitted to an Unavailable Routed Service.	30 min
CARxDiscUnexpEvent	Number of ingress events discarded because it was unexpected in the connection operational state.	30 min
CARxDscrdBundle	Number of ingress bundled event discarded during de-serialization	30 min
CARxDscrdConnUnavail	Number of User Data ingress events discarded because connection was not in-service.	30 min
CARxDscrdDecodeFailed	Number of ingress events discarded because failed to deserialize (event not part of stack service language).	30 min
CARxDscrdIncompat	Number of ingress events discarded because an Incompatible header version is received.	30 min
CARxDscrdInternalErr	Number of ingress events discarded because of other unexpected internal processing error.	30 min

Measurement Tag	Description	Collection Interval
CARxDscrdLayerSendFail	Number of User Data ingress events discarded because layer's sendTo failed.	30 min
CARxDscrdMsgLenErr	Number of ingress events discarded as it doesn't contain enough bytes (less than event header bytes).	30 min
CARxDscrdUnkServer	Number of ingress events discarded because the origination server was unknown/not configured.	30 min
CARxDscrdUnkStkLyr	Number of User Data ingress events discarded because stack layer is not known.	30 min
CARxMsgUnknown	Number of ingress events discarded because stack event was unknown.	30 min
CAStackQueueFul	StackEvents discarded due to ComAgent task queue full condition.	30 min
CATransDscrdInvCorrId	Number of received stack events that were received and discarded because they did not correlate with a pending transaction.	30 min
CATransDscrdStaleErrRsp	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.	30 min
CATransEndAbnorm	Number of reliable transactions that terminated abnormally.	30 min
CATransEndAbnormRateAvg	Average rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndAbnormRateMax	Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndAnsErr	Number of reliable transactions initiated by local User Layers that ended with an error response from a destination server.	30 min
CATransEndErr	Number of reliable transactions initiated by local User Layers that ended abnormally with an error response from a destination server.	30 min
CATransEndNoResources	Number of reliable transactions initiated by local User Layers that ended abnormally due to lack of resources.	30 min

Measurement Tag	Description	Collection Interval
CATransEndNoResponse	Number of reliable transactions initiated by local User Layers that ended abnormally due to a timeout waiting for a response.	30 min
CATransEndUnkwnSvc	Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to an unknown service.	30 min
CATransEndUnregSvc	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.	30 min
CATransNoReTxMaxTTL	Number of reliable transactions abnormally ended because of Max Time to live exceeded without any retransmits.	30 min
CATransRetx	Number of times stack events were retransmitted.	30 min
CATransReTxExceeded	Number of reliable transactions abnormally ended because of Max number of Retries exceeded.	30 min
CATransStaleSuccessRsp	Number of times that a success response was received from an unexpected server and was accepted to end a transaction.	30 min
CATransTTLExceeded	Number of reliable transactions abnormally ended because of Max Time to live exceeded.	30 min
CATxDscrdConnUnAvail	Number of User Data egress events discarded because connection was not in-service(down/blocked/not aligned).	30 min
CATxDscrdDestUserIncmpat	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)	30 min
CATxDscrdEncodeFail	Number of User Data egress events discarded because of serialization failures	30 min
CATxDscrdInternalErr	Number of egress events discarded because of other unexpected internal processing error.	30 min
CATxDscrdMxSendFail	Number of User Data egress events discarded because of failure reported by MxEndpoint	30 min
CATxDscrdUnknownSvc	Number of non-reliable and non-request (G=0 or R=0) egress stack events discarded because they refer to an unknown service.	30 min

Measurement Tag	Description	Collection Interval
CATxDscrdUnkServer	Number of egress events discarded because the destination server was unknown/not configured.	30 min
CATxDscrdUnregSvc	Number of egress stack events discarded because they reference a known service that has no registered User Layer.	30 min

CADDataFIFOQueueFul

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

1. When this measurement is increasing, it is an indication that the product is experiencing overload. 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.

CAHSRsrcErr

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (by Resource ID)
Description	Number of times that ComAgent receives in a heartbeat stack event status concerning a known Resource but an unknown Sub-Resource.
Collection Interval	30 min
Peg Condition	When ComAgent stores an unexpected Sub-Resource entry in the local Resource Provider Table. An unexpected Sub-Resource involves a known Resource but an unknown Sub-Resource ID (SRID). This condition is associated with Alarm-ID 19848, and only the first instance of an unexpected Sub-Resource is counted, not the repeats caused by multiple unknown Sub-Resources and the periodic heartbeats containing the same information.
Measurement Scope	Server

Recovery

1. Use **Main Menu > Communication Agent > Maintenance** to determine configuration problems.
2. Contact [My Oracle Support \(MOS\)](#) for assistance.

CAHSTxDscrdCongSR

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.

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 \(MOS\)](#).

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 > Communication 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 > Communication 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.	
2.	Use Main Menu > Communication Agent > Maintenance > HA Services Status to verify that all HA Service Sub-Resources expected by local applications are present and operating.
3.	Contact My Oracle Support (MOS) for assistance.

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.

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.

CAPSTxDscrdUnkwnGrp

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of egress stack events discarded because they referred to a Peer Group which was unknown
Collection Interval	30 min
Peg Condition	For each stack event submitted to ComAgent by a local User Layer and the stack event reference an Unknown Peer Group
Measurement Scope	Server

Recovery

1. A non-zero value of this measurement indicates that a local User Layer is malfunctioning and is attempting to use a Peer Group which it has not configured.
2. Contact [My Oracle Support \(MOS\)](#) for assistance.

CAPSTxDscrdUnavailGrp

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (by Peer Group ID)

Description	The number of egress stack events discarded because they referred to a Peer Group which was unavailable
Collection Interval	30 min
Peg Condition	For each stack event submitted to ComAgent by a local User Layer and the stack event reference an Unavailable Peer Group
Measurement Scope	Server

Recovery

- Each count of this measurement indicates that a local User Layer attempted to send a stack event to a remote server using ComAgent Peer Group Service, but the event was discarded due to the specified Peer Group being unavailable. The Peer Group may become unavailable due to:
 - Local User Layer performed maintenance action on the Peer Group that result in a loss of communication between servers.
 - Network problems that result in a loss of communication between servers.
- Contact [My Oracle Support \(MOS\)](#) for assistance.

CAPSTxDscrdCongPeer

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (by Peer Group ID)
Description	The number of egress stack events discarded because of Peer congestion.
Collection Interval	30 min
Peg Condition	For each stack event submitted to ComAgent by a local User Layer and the active Peer in the Peer Group has a congestion level greater than the priority level of the stack event.
Measurement Scope	Server

Recovery

- 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.
- 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	<p>This value provides a measure of how many times pre-allocated resources are exhausted in ComAgent interfaces.</p> <p>This measurement is primarily intended for performance analysis and to assist in evaluating the need for any additional engineering processing capacity or tuning.</p>

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 Router 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. Note: 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: <ul style="list-style-type: none"> • 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.
Measurement Scope	Server
Recovery	<ol style="list-style-type: none"> 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.

CARxDscrdBundle

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of ingress bundled event discarded during routing.
Collection Interval	30 min
Peg Condition	Each time an ingress bundled event is discarded during routing
Measurement Scope	Site

Recovery

No action required

CARxDscrdConnUnavail

Measurement Group	ComAgent Exception
--------------------------	--------------------

Measurement Type	Simple
Measurement Dimension	
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.

CASStackQueueFul

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	<p>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. 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:</p> <ul style="list-style-type: none"> • Network problems result in intermittent loss of communication between servers. • Server overload results in delayed responses

Measurement Scope Server

Recovery

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	<ul style="list-style-type: none"> • 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. <p>Note: This measurement is NOT pegged for these conditions:</p> <ul style="list-style-type: none"> • 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. 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.
Measurement Scope	Server
Recovery	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. 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.
Measurement Scope	Server
Recovery	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. 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.
Measurement Scope	Server
Recovery	<ol style="list-style-type: none"> 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. 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.

Measurement Scope Server

Recovery

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. 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.

Measurement Scope Server

Recovery

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. This measurement indicates improper configuration of ComAgent and/or a User Layer application.
Measurement Scope	Server

Recovery

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. 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: <ul style="list-style-type: none"> • Server overload that can result in delayed responses. • Unexpected conditions in software.
----------------------	--

Measurement Scope	Server
--------------------------	--------

Recovery

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. 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: <ul style="list-style-type: none"> • 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.

Measurement Scope	Server
--------------------------	--------

Recovery

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. 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: <ul style="list-style-type: none"> • Maintenance actions performed that result in a loss of communication between servers. • Server overload that can result in delayed responses. • Unexpected conditions in software.
Measurement Scope	Server

Recovery

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. 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.
Measurement Scope	Server

Recovery

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. 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: <ul style="list-style-type: none"> • Maintenance actions performed that result in a loss of communication between servers. • Server overload that can result in delayed responses. • Unexpected conditions in software.
Measurement Scope	Server

Recovery

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 Type	Simple
Measurement Dimension	Single
Description	Number of egress bundled event discarded during routing.
Collection Interval	30 min
Peg Condition	Each time an egress bundled event is discarded during routing
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
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	<ol style="list-style-type: none"> 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 20: Communication Agent Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
CAAvgDataFIFOQueueUtil	Average percentage of ComAgent DataFIFO Queue Utilization	30 min
CAAvgMxFIFOQueueUtil	Average percentage of ComAgent MxFIFO Queue Utilization	30 min
CAAvgQueueUtil	Average percentage of Queue Utilization.	30 min
CAAvgRsrcPoolUtil	Average percentage of internal resource pool utilization	30 min

Measurement Tag	Description	Collection Interval
CAAvgRxStackEvents	Average Number of User Data ingress events received.	30 min
CAAvgTxStackEvents	Average Number of User Data egress events received from stacks to deliver it to remote.	30 min
CADSTx	Number of User Data egress events specifically for the default Direct Service.	30 min
CAHSTxRsrc	Number of egress stack events that were routed to a known Resource.	30 min
CAHSTxRsrcRateAvg	Average rate per second of egress stack events routed to a known Resource.	30 min
CAHSTxRsrcRateMax	Maximum rate per second of egress stack events routed to a known Resource	30 min
CAPeakDataFIFOQueueUtil	Maximum percentage of ComAgent DataFIFO Queue Utilization	30 min
CAPeakMxFIFOQueueUtil	Maximum percentage of ComAgent MxFIFO Queue Utilization	30 min
CAPeakQueueUtil	Maximum percentage of Queue Utilization.	30 min
CAPeakRsrcPoolUtil	Maximum percentage of internal resource pool utilization	30min
CAPeakRxStackEvents	Maximum Number of User Data ingress events received.	30 min
CAPeakTxStackEvents	Maximum Number of User Data egress events received from stacks to deliver it to remote.	30 min
CAPSTxGrpSuccess	Number of egress stack events successfully routed to a known Peer Group.	30 min
CAPSTxGrp	Number of egress stack events submitted to the PG Service to be routed to a known Peer Group.	30 min
CARSTx	Number of stack events submitted to a Routed Service for routing.	30 min
CARx	Number of User Data ingress events received from a peer server.	30 min
CARxSuccess	Number of User Data ingress events successfully routed to local layers.	30 min
CATransEndAbnorm	Number of reliable transactions that terminated abnormally.	30 min

Measurement Tag	Description	Collection Interval
CATransEndAbnormRateAvg	Average rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndAbnormRateMax	Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndNorm	Number of reliable transactions initiated by local User Layers that ended normally with a response from a destination server.	30 min
CATransPendingAvg	Average number of allocated pending transaction records over the collection interval.	30 min
CATransPendingMax	Maximum number of allocated pending transaction records.	30 min
CATransRateAvg	Average rate per second that ComAgent transactions were started during the collection interval.	30 min
CATransRateMax	Maximum rate per second that ComAgent transactions were started during the collection interval.	30 min
CATransStarted	Number of reliable transactions initiated by local User Layers.	30 min
CATransTimeAvg	Average transaction life-time in milliseconds.	30 min
CATransTimeMax	Maximum transaction life-time in milliseconds.	30 min
CATx	Number of User Data egress events received on Communication Agent task queue from local stacks to deliver it to a peer server.	30 min
CATxSuccess	Number of User Data egress events successfully delivered to a peer server.	30 min

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 Performance
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. 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.
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.

CAPSTxGrp

Measurement Group	ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (by Peer Group ID)
Description	The number of egress stack events submitted to the Peer Group Service to be routed to a known Peer Group.
Collection Interval	30 min
Peg Condition	For each stack event submitted to ComAgent Peer Group Service by a local User Layer
Measurement Scope	Server
Recovery	No action required. This measurement is useful when compared with other Peer Group Service measurements.

CAPSTxGrpSuccess

Measurement Group	ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (by Peer Group ID)
Description	The number of egress stack events successfully routed to a known Peer Group.
Collection Interval	30 min
Peg Condition	For each stack event submitted to ComAgent Peer Group Service by a local User Layer and successfully routed
Measurement Scope	Server
Recovery	

No action required. This measurement is useful when compared with other Peer Group Service measurements.

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
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 Type	Simple
Measurement Dimension	Single
Description	Number of ComAgent Bundled events received by ComAgent
Collection Interval	30 min
Peg Condition	Each time a ComAgent Bundled event is received by ComAgent
Measurement Scope	Site
Recovery	No action required

CARxEventsBundled

Measurement Group	ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of stackevents received in ComAgent Bundled events
Collection Interval	30 min
Peg Condition	Each time a stackevent is received in ComAgent Bundled events
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	<ul style="list-style-type: none"> • 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. <p>Note: This measurement is NOT pegged for these conditions:</p> <ul style="list-style-type: none"> • 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. 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.
Measurement Scope	Server

Recovery

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. 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.
Measurement Scope	Server
Recovery	No action necessary.

CATransEndNorm

Measurement Group	ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (by Service ID)
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. 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.
Measurement Scope	Server
Recovery	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. 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.
Measurement Scope	Server
Recovery	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 Type	Simple
Measurement Dimension	Single
Description	Number of ComAgent Bundled events transmitted by ComAgent
Collection Interval	30 min
Peg Condition	Each time a ComAgent Bundled event is transmitted by ComAgent
Measurement Scope	Site
Recovery	No action required

CATxEventsBundled

Measurement Group	ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of stackevents transmitted through ComAgent Bundled events
Collection Interval	30 min
Peg Condition	Each time a stackevent is transmitted through ComAgent Bundled events
Measurement Scope	Site
Recovery	No action required

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.

HLR Measurements

This section provides information about HLR measurement reports.

EXHR measurements

Table 21: EXHR Measurement Report Fields

Measurement Tag	Description	Collection Interval
ExhrGttAlternateRoute	Number of GTTs performed where the preferred destination was not available	5 min
ExhrGttExceptionRouting	Number of times exception routing was used	5 min
ExhrGttFail	Number of Global Title Translation failures	5 min
ExhrGttFailIncorrectGTI	Number of Global Title Translation failures due to incorrect Global Title Indicator	5 min
ExhrGttFailNoTransForAddress	Number of Global Title Translation failures due to IMSI/DN not provisioned	5 min

Measurement Tag	Description	Collection Interval
ExhrGttFailTTNotFound	Number of Global Title Translation failures due to Translation Type not provisioned	5 min
ExhrGttPerformed	Number of Global Title Translations performed	5 min
ExhrGttExceptionRtgOverride	Total number of messages where Exception Routing was overridden	5 min
ExhrGttExceptionRtgOverrideErr	Total number of TCAP Response Failures when the Exception Routing Override feature is active and the response message fails during encode.	5 min
ExhrMlrDecodeFailed	Total number of messages that failed Map Layer Routing decode. HLRR failed to find IMSI/DN in the MAP layer.	5 min
ExhrMlrDecodeSuccessful	Total number of messages that were successfully Map Layer Decoded. HLRR found IMSI/DN in the MAP Layer.	5 min
ExhrMlrFailNoTransForAddress	Total number of MLR failures due to IMSI/DN not provisioned. IMSI/DN found in MAP Layer but not in Database.	5 min
ExhrMlrPerformed	Total number of messages that were MLR Performed. IMSI/DN found in MAP Layer and in Database plus the message was successfully routed.	5 min

EXHRTT measurements

Table 22: EXHRTT Measurement Report Fields

Measurement Tag	Description	Collection Interval
ExhrGttFailNoTransForAddressByTT	Number of Global Title Translation failures due to IMSI/DN not provisioned, by TT	5 min

Measurement Tag	Description	Collection Interval
ExhrGttPerformedByTT	Number of Global Title Translations performed, by TT	5 min
ExhrGttFailTTNotFoundByTT	Total number of GTT failures due to translation type not provisioned, per translation type	5 min

PDBI measurements

Table 23: PDBI Measurement Report Fields

Measurement Tag	Description	Collection Interval
NetSync RepAud ErrCnt	Number of errors detected	5 min
NetSync RepAud RecCnt	Number of records audited	5 min
PdbiConnectionIdleTimeouts	Total number of connections that have timed out and terminated due to idleness.	5 min
PdbiConnectsAccepted	Total number of client initiated connect attempts that have been accepted.	5 min
PdbiConnectsAttempted	Total number of client initiated connect attempts to establish a connection with the server.	5 min
PdbiConnectsDenied	Total number of client initiated connect attempts that have been denied due to clients not running on an authorized server, maximum number of allowed connections already established, or the PDBI interface is disabled.	5 min
PdbiConnectsFailed	Total number of client initiated connect attempts that failed due to errors during initialization.	5 min
PdbiDnSplitCreated	Number of DN records created by NPA split	5 min
PdbiDnSplitRemoved	Number of DN records removed by NPA split	5 min
PdbiEpapAuditCompleted	Number of completed EPAP audits	5 min
PdbiEpapAuditStarted	Number of started EPAP audits	5 min

Measurement Tag	Description	Collection Interval
PdbiExportsFailed	Total number of PDBI export requests that have failed due to errors.	5 min
PdbiExportsSuccessful	Total number of successful PDBI export requests.	5 min
PdbiImportsFailed	Total number of files that had failed to be imported to PDBI due to errors.	5 min
PdbiImportsSuccessful	Total number of files imported to PDBI successfully.	5 min
PdbiMsgsDiscarded	The total number of PDBI messages that have been discarded due to the connection being shutdown, server being shutdown, server's role switching from active to standby, or transaction not becoming durable within the allowed amount of time.	5 min
PdbiMsgsFailed	The total number of PDBI messages that have failed to be processed due to errors. See section 5.1 for a list and description of possible errors.	5 min
PdbiMsgsImported	The total number of PDBI messages that have been received from an import operation.	5 min
PdbiMsgsReceived	The total number of PDBI messages that have been received.	5 min
PdbiMsgsSent	The total number of PDBI messages that have been sent.	5 min
PdbiMsgsSuccessful	The total number of PDBI messages that have been successfully processed.	5 min
PdbiNpaSplitCompleted	Number of completed NPA splits	5 min
PdbiNpaSplitStarted	Number of started NPA splits	5 min
PdbiTxnAborted	Total number of transactions that have been successfully aborted.	5 min

Measurement Tag	Description	Collection Interval
PdbiTxnCommitted	The total number of transactions that have been successfully committed to the database (memory and on disk) on the active server of the primary NOAM cluster.	5 min
PdbiTxnDurabilityTimeouts	The total number of committed, non-durable transaction that have failed to become durable within the amount of time specified by Transaction Durability Timeout.	5 min
PdbiTxnFailed	Total number of transactions that have failed to be started, committed, or aborted due to errors.	5 min
PdbiTxnTimeouts	Total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.	5 min
PdbiTxnTotal	Total number of transactions that have been attempted. It is the sum of pdbi.TxnCommitted, pdbi.TxnTimeouts, pdbi.TxnAborted, and pdbi.TxnFailed counters.	5 min
PdbiTxnWriteMutexTimeouts	The total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.	5 min

PDE measurements

Table 24: PDE Measurement Report fields

Measurement Tag	Description	Collection Interval
PdeFilesCreatedNO	Number of created files on NOAM server	5 min
PdeFilesTransferredNO	Number of transferred files from NOAM server	5 min

Measurement Tag	Description	Collection Interval
PdeFilesCreatedSO	Number of created files on SOAM server	5 min
PdeFilesTransferredSO	Number of transferred files from SOAM server	5 min

OAM measurements

This section describes the OAM measurement reports. These measurements provide information about OAM system and alarm measurements. The measurements in this section are available in all Tekelec XG products.

OAM.ALARM measurements

Table 25: OAM Alarm Measurements

Measurement Tag	Description	Collection Interval
Alarm.Crit	The number of critical alarms.	5 minutes
Alarm.Major	The number of major alarms.	5 minutes
Alarm.Minor	The number of minor alarms	5 minutes
Alarm.State	The alarm state.	5 minutes

OAM.SYSTEM measurements

Table 26: OAM System Measurements

Measurement Tag	Description	Collection Interval
System.CPU_UtilPct_Average	The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System.CPU_UtilPct_Peak	The peak CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System.Disk_UtilPct_Average	The average disk usage for the partition on which the COMCOL database resides.	5 minutes
System.Disk_UtilPct_Peak	The peak disk usage for the partition on which the COMCOL database resides.	5 minutes
System.RAM_UtilPct_Average	The average committed RAM usage as a percentage of the total physical RAM. This	5 minutes

Measurement Tag	Description	Collection Interval
	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.	
System.RAM_UtilPct_Peak	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.	5 minutes
System.ShMem_UtilPct_Average	The average shared memory usage as a percentage of the limit configured by shl.set.	5 minutes
System.ShMem_UtilPct_Peak	The peak shared memory usage as a percentage of the limit configured by shl.set.	5 minutes
System.SwapIn_Rate_Average	The average number of memory pages swapped in to memory from disk per second.	5 minutes
System.SwapIn_Rate_Peak	The peak number of memory pages swapped in to memory from disk per second.	5 minutes
System.SwapOut_Rate_Average	The average number of memory pages swapped out of memory from disk per second.	5 minutes
System.SwapOut_Rate_Peak	The peak number of memory pages swapped out of memory from disk per second.	5 minutes
System.Swap_UtilPct_Average	The average usage of swap space as a percentage of the total configured swap space.	5 minutes
System.Swap_UtilPct_Peak	The peak usage of swap space as a percentage of the total configured swap space.	5 minutes
System.CPU_CoreUtilPct_Average	The average CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.	5 minutes

Measurement Tag	Description	Collection Interval
System.CPU_CoreUtilPct_Peak	The peak CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.	5 minutes

SS7/Sigtran Measurements

This section provides information about SS7/Sigtran measurement reports and detailed information about each measurement.

SS7/Sigtran measurements overview

SS7/Sigtran signaling measurements provide information about SCCP functionality, MTP3 routing capabilities, and the M3UA interface to the external network and can alert you to SS7/Sigtran issues before an alarm or event is triggered. This section of the documentation provides overview information about SS7/Sigtran measurement reports and detailed information about each measurement on the report, including potential customer actions.

Association Exception measurements

Table 27: Association Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxTrFarEndClose	Number of times the far end closed the SCTP connection.	30 min
EvTrManClose	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.	30 min
EvTrNoRespClose	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.	30 min
EvTrCnxFail	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.	30 min

Measurement Tag	Description	Collection Interval
TxTrSendFail	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.	30 min
RxTrRcvFail	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.	30 min
EvTrSockInitFail	Number of times the socket initialization failed.	30 min
RxM3uaERROR	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.	30 min
TmSingleTransQueueFull	The number of egress messages that were discarded because the single Transport Writer Queue was full.	30 min
EvAsnUpAckTO	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).	30 min
RxAsnUnsolDownAck	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.	30 min
RxAsnInvalidM3ua	Number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.	30 min
EvSctpAdjIPToDwn	Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.	30 min
EvSctpTransRej	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.	30 min

RxAsnFarEndClose

Measurement Group

Association Exception

Measurement Type

Simple

Measurement Dimension	Arrayed (per association)
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.

EvAsnManClose

Measurement Group	Association Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (per association)
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.

EvAsnNoRespClose

Measurement Group	Association Exception
Measurement Type	Simple
Measurement Dimension	
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
Measurement Dimension	Arrayed (per Transport)
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.

TxAsnSendFail

Measurement Group Association Exception

Measurement Type Simple

Measurement Dimension Arrayed (per association)

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 - Failed to send non-DATA message. Refer to the *DSR Alarms and KPIs Reference* for details about this event and 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.

RxAsnRecvFailed

Measurement Group	Association Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (per association)
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	Transport Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (per Transport)
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
Measurement Dimension	Arrayed (per association)
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 ID19235 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
Measurement Dimension	Arrayed (per association)
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
Measurement Dimension	Arrayed (per association)
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
Measurement Dimension	Arrayed (per association)
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
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 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

Measurement Dimension	Arrayed (per Transport)
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 reachability to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected. 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.
Measurement Scope	NE, Server

Recovery

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
Measurement Dimension	Arrayed (per Transport)
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. 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.
Measurement Scope	NE, Server

Recovery

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 28: Association Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxTrOctets	The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min
RxTrOctets	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min
SCTPAssocQueuePeak	The peak SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.	30 min
SCTPAssocQueuePeak	The average SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.	30 min

TxTrOctets

Measurement Group	Association Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (per Transport)
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	Association 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	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
Measurement Dimension	Arrayed
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.
3. See Alarm 19408 - Single Transport Egress-Queue Utilization (refer to the *DSR Alarms and KPIs Reference* for details about this alarm).
4. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

SCTPAssocQueueAvg

Measurement Group	Association Performance
--------------------------	-------------------------

Measurement Type	Average
Measurement Dimension	Arrayed
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 29: Association Usage Measurement Report Fields**

Measurement Tag	Description	Collection Interval
EvTrCnxSuccess	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.	30 min
TmAsnBlkNotDown	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.	30 min
RxTrOctets	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min

EvAsnCnxSuccess

Measurement Group Association Exception

Measurement Type	Simple
Measurement Dimension	Arrayed (per association)
Description	The number of times the SCTP connection was successfully established on the association.
Collection Interval	30 min
Peg Condition	This measurement shall be incremented by one each time the SCTP association reaches the ASP-DOWN protocol state (for example, the connection is successfully established).
Measurement Scope	NE, Server

Recovery

1. If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise, perform the following steps:
2. You can view the transport status can be viewed from the GUI main menu under **Transport Manager > Maintenance > Transport**.
3. 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.
4. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

TmAsnBlkNotDown

Measurement Group	Association Usage
Measurement Type	Duration
Measurement Dimension	Arrayed (per association)
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: <ul style="list-style-type: none"> • 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 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 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
Measurement Dimension	Arrayed (per association)
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: <ul style="list-style-type: none"> • 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 30: Link Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvLnkActAckTO	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.	30 min
RxLnkUnsollnactAck	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.	30 min

Measurement Tag	Description	Collection Interval
	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.	
RxLnkM3uaERROR	Number of times an M3UA ERROR message was received for the link. M3UA ERROR message are sent to indicate invalid M3UA signaling.	30 min
RxLnkInvalidM3ua	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).	30 min

EvLnkActAckTO

Measurement Group	Link Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (per link)
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.

RxLnkUnsolicitedAck

Measurement Group	Link Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (per link)
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
Measurement Dimension	Arrayed (per link)
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
Measurement Dimension	Arrayed (per link)
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 31: Link Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxLnkMSU	Number of MSUs sent on the link. MSUs includes all M3UA messages, both DATA and non-DATA.	30 min

Measurement Tag	Description	Collection Interval
RxLnkMSU	Number of MSUs received on the link. MSUs includes all M3UA messages, both DATA and non-DATA.	30 min
TxLnkMSUOctets	Number of MSU octets sent on the link. MSU octets includes all M3UA messages, both DATA and non-DATA.	30 min
RxLnkMSUOctets	Number of MSU octets received on the link. MSU octets includes all M3UA messages, both DATA and non-DATA.	30 min

TxLnkMSU

Measurement Group	Link Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (per link)
Description	<p>The number of MSUs sent on the link, including all M3UA messages, both DATA and non-DATA.</p> <p>Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.</p>
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
Measurement Dimension	Arrayed (per link)
Description	<p>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.</p>
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
Measurement Type	Arrayed (per link)
Measurement Dimension	Simple
Description	The number of MSU octets 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 the number of octets in the MSU (not including SCTP, IP, or Ethernet headers) each time an M3UA message is sent on the link.
Measurement Scope	NE, Server
Recovery	No action required.

RxLnkMSUOctets

Measurement Group	Link Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (per link)
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 32: Link Set Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxLnkSetMSU	Number of MSUs sent on the link set. MSUs includes all M3UA DATA messages sent on all links in the link set.	30 min
RxLnkSetMSU	Number of MSUs received on the link set. MSUs includes all M3UA DATA messages received on all links in the link set.	30 min
TxLnkSetMSUOctets	Number of MSU octets sent on the link set. MSU octets includes all M3UA DATA octets sent on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.	30 min
RxLnkSetMSUOctets	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.	30 min

TxLnkSetMSU

Measurement Group	Link Set Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (per link set)
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
Measurement Dimension	Arrayed (per link set)
Description	The number of MSUs sent on the link set, including 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
Measurement Dimension	Arrayed (per link set)
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
Measurement Dimension	Arrayed (per link set)
Description	The number of MSU octets received on the link set, including 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 33: Link Set Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
TmM3RLLinksetUnavail	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.	30 min

TmM3RLLinksetUnavail

Measurement Group Link Set Usage

Measurement Type Duration

Measurement Dimension Arrayed (by Linkset)

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 (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) 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

Recovery

This value provides a measure of the availability of a Link Set. No action required.

Link Usage measurements

Table 34: Link Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
TmLnkMOOS	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.	30 min
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: <ul style="list-style-type: none"> • Maintenance activity: link is Disabled or the 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. • A 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. 	30 min
TmLnkAvailable	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.	30 min
EvLnkManClose	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 Enabled to Disabled .	30 min

TmLnkMOOS

Measurement Group	Link Usage
Measurement Type	Duration
Measurement Dimension	Arrayed (per link)
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 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.

Peg Condition 30 min

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**.
2. Also, look in the GUI main menu under **Alarms & Events > View History** in the event history for Event 19234 - Local link maintenance state change (refer to the *DSR Alarms and KPIs Reference* for details about this event). 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

Measurement Dimension Arrayed (per link)

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
Measurement Dimension	Arrayed (per link)
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 **TmLnkMOOS** and **TmLnkOOS** should have a non-zero values. See the actions for [TmLnkMOOS](#).
 - Link failure. The measurement **TmLnkOOS** should have a non-zero value. See the actions for [TmLnkOOS](#).
 - The link was added during the reporting period. The report indicates that the data is incomplete for the reporting period.
2. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

EvLnkManClose

Measurement Group	Link Usage
Measurement Type	Simple
Measurement Dimension	
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 Enabled to Disabled
Collection Interval	30 min
Peg Condition	This measurement is incremented by one each time the link administrative state is changed from Enabled to Disabled , causing a protocol state transition from ASP-ACTIVE to ASP-INACTIVE.
Measurement Scope	NE, Server

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 [My Oracle Support \(MOS\)](#) for assistance if needed.

Server M3UA Exception measurements**Table 35: Server M3UA Exception Measurement Report Fields**

Measurement Tag	Description	Collection Interval
TxM3uaERROR	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.	30 min
RxM3uaERROR	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.	30 min
M3UAStackQueueFull	Number of messages that were discarded because the M3UA Stack Event Queue was full	30 min
SCTPAggrQueueFull	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.	30 min
ANSIDiscardsNoPDUBuffer	ANSI ingress message discarded: no PDU buffer.	30 min
ITUDiscardsNoPDUBuffer	The number of ingress messages that were discarded because no ITU/ITUN PUD Buffers were available.	30 min

TxM3uaERROR**Measurement Group**

Server M3UA Exception

Measurement Type

Simple

Measurement Dimension	Single
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**, which 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
Measurement Dimension	Single
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. 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 19235, which provides details about the reason for sending the M3UA ERROR message.
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.

M3UAShouldQueueFull

Measurement Group	Server M3UA Exception
Measurement Type	Simple
Measurement Dimension	Single
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
Peg Condition	Each time a M3UA Stack Event Queue message is discarded
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.

SCTP AggrQueueFull

Measurement Group	Server M3UA Exception
Measurement Type	Simple
Measurement Dimension	Single
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	Each time a SCTP Aggregate Association Writer Queue message is 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 \(MOS\)](#).

ANSIDiscardsNoPDUBuffer

Measurement ID	9245
Measurement Group	Server M3UA Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of ingress ANSI messages that were discarded because no ANSI PDU Buffers were available.
Collection Interval	30 min
Peg Condition	Each time an ANSI message is 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 \(MOS\)](#).

ITUDiscardsNoPDUBuffer

Measurement ID	9245
Measurement Group	Server M3UA Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of ingress messages that were discarded because no ITUI/IITUN PDU Buffers were available.
Collection Interval	30 min
Peg Condition	Each time an ITUI message is 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 \(MOS\)](#).

ItunRxNoPDUBuffer

Measurement Group	Server M3UA Exception
Measurement Type	Simple
Measurement Dimension	Single
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, it is recommended to contact [My Oracle Support \(MOS\)](#).

Server M3UA Performance measurements**Table 36: Server M3UA Performance Measurement Report Fields**

Measurement Tag	Description	Collection Interval
TxNonDataMsg	Non-DATA messages 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.	30 min
RxNonDataMsg	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.	30 min
TxNonDataOctets	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.	30 min
RxNonDataOctets	Non-DATA octets received by the MP server. This includes all non-DATA M3UA messages	30 min

Measurement Tag	Description	Collection Interval
	(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.	
M3UAShouldQueuePeak	Peak M3UA Network Management Event Queue utilization (0-100%) measured during the collection interval.	30 min
M3UAShouldQueueAvg	Average M3UA Stack Event Queue utilization (0-100%) measured during the collection interval.	30 min
SCTPAggrQueuePeak	Peak SCTP Aggregate Association Writer Queue utilization (0-100%) measured during the collection interval.	30 min
SCTPAggrQueueAvg	Average of all SCTP Aggregate Association Writer Queue utilization samples taken during the collection interval.	30 min

TxNonDataMsg

Measurement Group	Server M3UA Performance
Measurement Type	Simple
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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

Measurement Dimension Single

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.

M3UAShouldQueuePeak

Measurement Group Server M3UA Performance

Measurement Type Max

Measurement Dimension Single

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.

M3UAShouldQueueAvg

Measurement Group Server M3UA Performance

Measurement Type Average

Measurement Dimension Single

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
Measurement Dimension	Single
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
Measurement Dimension	Single
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 37: Server M3UA Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxASPSM	Number of ASPSM messages sent by the MP server.	30 min
RxASPSM	Number of ASPSM messages received by the server.	30 min
TxASPTM	Number of ASPTM messages sent by the MP server.	30 min
RxASPTM	Number of ASPTM messages received by the MP server.	30 min
TxDAUD	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.	30 min
RxSSNM	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.	30 min

Measurement Tag	Description	Collection Interval
RxM3uaNOTIFY	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.	30 min

TxASPSM

Measurement Group	Server M3UA Usage
Measurement Type	Simple
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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

Measurement Dimension	Single
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.

RxSSNM

Measurement Group	Server M3UA Usage
Measurement Type	Simple
Measurement Dimension	Single
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: <ul style="list-style-type: none"> • 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
Measurement Dimension	Single

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 38: Server MTP3 Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxM3RLDestUnknown	Number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.	5 min
TxM3RLDestUnavail	Number of egress messages M3RL discarded because the RSP/Destination was Unavailable.	5 min
TxM3RLDestCong	Number of egress messages M3RL discarded because the RSP/Destination's congestion level was higher than the message's priority.	5 min
TxM3RLBufOverflow	Number of egress messages M3RL discarded because of an internal buffer overflow.	5 min
RxM3RLInvalidDPC	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.	5 min
RxM3RLInvalidSI	Number of ingress messages M3RL discarded because the Service Indicator received was not 0 (SNM) or 3 (SCCP).	5 min
RxM3RLInvalidNI	Number of ingress messages M3RL discarded because the Network Indicator received was not the same value configured for the MP.	5 min
RxM3RLBufOverflow	Number of ingress messages M3RL discarded because of an internal buffer overflow.	5 min

Measurement Tag	Description	Collection Interval
M3RLStackQueueFull	Number of messages that were discarded because the M3RL Stack Event Queue was full.	5 min
M3RLNetMgtQueueFull	Number of M3RL network management messages (SI=0) that were discarded because the M3RL Network Management Event Queue was full.	5 min

TxM3RLDestUnknown

Measurement Group	Server MTP3 Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of egress messages M3RL discarded because no routing information exists for the RSP/Destination.
Collection Interval	5 min
Peg Condition	For each message discarded
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
Measurement Dimension	Single
Description	The number of egress messages M3RL discarded because the RSP/Destination was Unavailable.
Collection Interval	5 min
Peg Condition	For each message discarded
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
Measurement Dimension	Single
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
Peg Condition	For each message discarded
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
Measurement Dimension	Single
Description	The number of egress messages M3RL discarded because of an internal buffer overflow.
Collection Interval	5 min
Peg Condition	For each message discarded
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
Measurement Dimension	Single

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	
Peg Condition	For each message discarded
Measurement Scope	NE, Server

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
Measurement Dimension	Single
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
Peg Condition	For each message discarded
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
Measurement Dimension	Single
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
Peg Condition	For each message discarded
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
Measurement Dimension	Single
Description	This value provides a measure of how many ingress messages M3RL discarded because of an internal buffer overflow.
Collection Interval	5 min
Peg Condition	For each message discarded
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
Measurement Dimension	Single
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
Peg Condition	For Each M3RL Stack Event Queue message is discarded
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
Measurement Dimension	Single
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
Peg Condition	Each time an M3RL Network Management Even Queue message is discarded
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 39: Server MTP3 Performance Measurement Report Fields**

Measurement Tag	Description	Collection Interval
TxM3RLDataMsgs	Egress M3RL DATA Messages (at M3RL->M3UA interface). This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SNM messages.	5 min
RxM3RLDataMsgs	Ingress M3RL DATA Messages (at M3RL->M3UA interface). This measurement includes SCMG messages (which are DATA to the M3RL layer), but does not include SSNM messages.	5 min
M3RLStackQueuePeak	Peak M3RL Stack Event Queue utilization (0-100%) measured during the collection interval	5 min
M3RLStackQueueAvg	Average M3RL Stack Event Queue utilization (0-100%) measured during the collection interval.	5 min
M3RLNetMgtQueuePeak	Peak M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval	5 min

Measurement Tag	Description	Collection Interval
M3RLNetMgtQueueAvg	Average M3RL Network Management Event Queue utilization (0-100%) measured during the collection interval	5 min

TxM3RLDataMsgs

Measurement Group	Server MTP3 Performance
Measurement Type	Simple
Measurement Dimension	Single
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
Measurement Dimension	Single
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
Peg Condition	This counter is pegged each time a M3RL DATA message is receive at M3RL from M3UA. This counter includes SCMG messages (which are DATA to the M3RL layer), but does not include SSNM messages.
Measurement Scope	NE, Server
Recovery	No action required.

M3RLStackQueuePeak

Measurement Group	Server MTP3 Performance
Measurement Type	Max
Measurement Dimension	Single
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.
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. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

M3UAStackQueueAvg

Measurement Group	Server M3UA Performance
Measurement Type	Average
Measurement Dimension	Single
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
Measurement Dimension	Single
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
Measurement Dimension	Single
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 40: Server Resource Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
SS7ProcessPeak	Peak SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.	5 min
SS7ProcessAvg	Average SS7 Process CPU utilization (0-100%) measured during the collection interval. The SS7 process is responsible for all SS7-related processing.	5 min
SS7RxMsgRatePeak	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.	5 min
SS7RxMsgRateAvg	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.	5 min
ITUPDUUtilPeak	The peak ITUI/ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
ITUPDUUtilAvg	The average ITUI/ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
ANSIPDUUtilPeak	The peak ANSI PDU Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
ANSIPDUUtilAvg	The average ANSI PDU Buffer Pool utilization (0-100%) measured during the collection interval.	5 min

SS7ProcessPeak

Measurement Group	Server Resource Usage
Measurement Type	Max
Measurement Dimension	Single
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
Measurement Dimension	Single
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
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 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
Measurement Dimension	Single
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.

ANSIPDUUtilPeak

Measurement ID	9243
Measurement Group	Server Resource Usage
Measurement Type	Max
Measurement Dimension	Single
Description	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 ID	9244
Measurement Group	Server Resource Usage
Measurement Type	Average
Measurement Dimension	Single
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.

ItuiPDUUtilPeak

Measurement Group	Server Resource Usage
Measurement Type	Max
Measurement Dimension	Single
Description	The peak SS7 ITUI PDU Buffer Pool utilization (0-100%) measured during the collection interval.
Collection Interval	5 min
Peg Condition	The maximum SS7 ITUI 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. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

ItuiPDUUtilAvg

Measurement Group	Server Resource Usage
--------------------------	-----------------------

Measurement Type	Average
Measurement Dimension	Single
Description	The average SS7 ITUI PDU Buffer Pool utilization (0-100%) measured during the collection interval.
Collection Interval	5 min
Peg Condition	The average of all SS7 ITUI 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. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

ItunPDUUtilPeak

Measurement Group	Server Resource Usage
Measurement Type	Max
Measurement Dimension	Single
Description	The peak SS7 ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.
Collection Interval	5 min
Peg Condition	The maximum SS7 ITUN PDU Buffer Pool utilization sample taken during the collection interval.
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.

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

ItunPDUUtilAvg

Measurement Group	Server Resource Usage
Measurement Type	Max
Measurement Dimension	Single
Description	The average SS7 ITUN PDU Buffer Pool utilization (0-100%) measured during the collection interval.
Collection Interval	5 min
Peg Condition	The average of all SS7 ITUN PDU Buffer Pool utilization sample taken during the collection interval.
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.
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. It is recommended to contact [My Oracle Support \(MOS\)](#) for assistance if needed.

Server SCCP Exception measurements

Table 41: Server SCCP Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvError	Number of error log events.	30 min

Measurement Tag	Description	Collection Interval
EvVital	Number of vital log events.	30 min
RxSCCPInvalidDPC	Number of ingress messages SCCP discarded because the DPC is not the TPC or CPC of an MP for an ingress SCCP message.	30 min
RxSCCPInvalidSSN	Number of ingress messages SCCP discarded because the CdPA SSN or affected SSN is missing/invalid for an ingress SCCP message.	30 min
RxSCCPInvalidMsg	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: SSA, SSP, SST.	30 min
RxSCCPInvalidHop	Number of ingress messages SCCP discarded because of a Hop Counter violation associated with CdPA RI=route on GT.	30 min
RxSCCPInvalidClass	Number of ingress messages SCCP discarded because of an invalid protocol class. Note: Only classes 0 and 1 are supported.	30 min
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 AWSS7 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

Measurement Tag	Description	Collection Interval
TxSCCPInvalidSSN	Number of egress messages SCCP discarded because the remote SSN is missing or invalid for an egress SCCP message.	30 min
SCCPStackQueueFull	Number of ingress SCCP messages that were discarded because the SCCP Stack Event Queue was full.	30 min
TxSCCPUnavailDPC	RSP/affected DPC unavailable for an egress SCCP message.	30 min
TxSCCPUnknownDPC	RSP/affected DPC unknown (unequipped) for an egress SCCP message.	30 min
TxSCCPUnavailSSN	Remote/affected SSN unavailable for an egress SCCP message.	30 min
TxSCCPUnknownSSN	Remote/affected SSN unknown (unequipped) for an egress SCCP message.	30 min
TxSCCPInvUserMsgs	Invalid N-UnitDatareq received from the Local SCCP User/application.	30 min
RxSCCPUnavailSSN	Messages received for a prohibited Local/Affected SSN.	30 min
RxSCCPUnknownSSN	Messages received for an unequipped/unknown Local/Affected SSN.	30 min
SCMGErrors	Number of ingress/egress malformed or unsupported messages.	30 min
SCCPGTTFailure	Default action for ri=rt-on-gttmessages from the SS7 stack.	30 min

EvError

Measurement ID 9901

Measurement Group Server SCCP Exception

Measurement Type Simple

Measurement Dimension Single

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

Peg Condition	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 ID	9900
Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single

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

Peg Condition	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
Measurement Dimension	Single

Description The number of ingress SCCP messages that were discarded because of the Local MP Maximum TPS limit.

Collection Interval	30 min
Peg Condition	For each message discarded
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 > 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 the GUI main menu 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. 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
Measurement Dimension	Single
Description	The number of ingress SCCP messages that were discarded because of local MP congestion.
Collection Interval	30 min
Peg Condition	For each message discarded
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 > 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 the GUI main menu under **Status & Control > 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. 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 ID	9055
Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
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
Peg Condition	For each message discarded
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 ID	9056
Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
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
Peg Condition	For each message discarded
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
Measurement Dimension	Single

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
Peg Condition	For each message discarded for an invalid Message Type
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
Measurement Dimension	Single
Description	Number of ingress messages SCCP discarded because of a Hop Counter violation associated with CdPA RI=route on GT.
Collection Interval	30 min
Peg Condition	For each message discarded
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
Measurement Dimension	Single
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
Peg Condition	For each message discarded for an invalid Protocol Class
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
Measurement Dimension	Single
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	For each message discarded
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
Measurement Dimension	Single
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
Measurement Dimension	Single

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
Measurement Dimension	Single
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
Measurement Dimension	Single
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

Measurement Dimension Single

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 a 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.

RxSCCPSgmntsPartReassFAIL

Measurement Group Server SCCP Exception

Measurement Type Simple

Measurement Dimension Single

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.

RxSCCPUnavailSSN

Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of ingress messages (RI=SSN) SCCP discarded because the CdPA SSN (Local SSN for MP's TPC) was manually disabled.
Collection Interval	30 min
Peg Condition	For each message discarded
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 GUI Main Menu: **SS7/SIGTRAN > Maintenance > Local SCCP Users**.

RxSCCPUnknownSSN

Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of ingress messages (RI=SSN) SCCP discarded because the CdPA SSN (Local SSN for MP's TPC) is not configured for the MTP DPC's signaling domain
Collection Interval	30 min
Peg Condition	For each message discarded
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 GUI Main Menu: **SS7/SIGTRAN > Configuration > Local SCCP Users [Insert]**.

RxSCCPXudtInvSgmt

Measurement Group	Server SCCP Exception
Measurement Type	Simple

Measurement Dimension	Single
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
Measurement Dimension	Single
Description	Count of SCCP GTT Failures due to default GTT handling in SS7Stack.
Collection Interval	30 min
Peg Condition	Default GTT Processing by SS7 Stack, when Application did not implement "rt-on-gt" message handling
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
Measurement Dimension	Single
Description	The number of ingress SCCP messages that were discarded because the SCCP Stack Event Queue was full.
Collection Interval	30 min
Peg Condition	For each message discarded
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
Measurement Dimension	Single
Description	Number of ingress/egress malformed or unsupported messages.
Collection Interval	30 min
Peg Condition	For each ingress/egress malformed or unsupported SCCP Management message
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
Measurement Dimension	Single
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
Peg Condition	For each message discarded
Measurement Scope	NE, Server

Recovery

You can view the remote RSPs/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
Measurement Dimension	Single
Description	SCCP User submitted an Invalid/malformed/unsupported message for egress routing (SCCP User->SCCP N-UnitDataReq)
Collection Interval	30 min
Peg Condition	For each message discarded
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.

TxSCCPInvalidDPC

Measurement ID	9051
Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
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
Peg Condition	For each message discarded
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.

TxSCCPInvalidSSN

Measurement ID	9052
Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
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

Peg Condition	For each message discarded
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
Measurement Dimension	Single
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
Measurement Dimension	Single
Description	Number of egress messages SCCP discarded because the affected DPC status was marked prohibited/unavailable.
Collection Interval	30 min
Peg Condition	For each message discarded
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 GUI Main Menu: **SS7/SIGTRAN > Maintenance > Remote Signaling Points.**

TxSCCPUnavailSSN

Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of egress messages SCCP discarded because the CdPA or Affected SSN was either marked prohibited/unavailable.
Collection Interval	30 min
Peg Condition	For each message discarded
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 GUI Main Menu: **SS7/SIGTRAN > Maintenance > Remote MTP3 Users.**

TxSCCPUnknownDPC

Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	Number of egress messages SCCP discarded because the affected DPC in message is not configured or is unknown.
Collection Interval	30 min
Peg Condition	For each message discarded
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 GUI Main Menu: **SS7/SIGTRAN > Maintenance > Remote Signaling Points.**

TxSCCPUnknownSSN

Measurement Group	Server SCCP Exception
Measurement Type	Simple
Measurement Dimension	Single

Description	Number of egress messages SCCP discarded because the CdPA or affected SSN was unknown.
Collection Interval	30 min
Peg Condition	For each message discarded
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 the GUI Main Menu: **SS7/SIGTRAN > Configuration > Remote MTP3 Users** and their status can be viewed via the GUI Main Menu: **SS7/SIGTRAN > Maintenance > Remote MTP3 Users**.

Server SCCP Performance measurements**Table 42: Server SCCP Performance Measurement Report Fields**

Measurement Tag	Description	Collection Interval
TxSCCPMsgs	Egress Messages Sent (to M3RL)	30 min
RxSCCPMsgs	Ingress Messages Received (from M3RL)	30 min
TxSCCPUserMsgs	Valid N-UnitDatareq generated by local SCCP User and processed by SCCP	30 min
TxSCMGMMsgs	Number of valid egress SCMG messages	30 min
RxSCCPUserMsgs	UDT/XUDT received and N-UnitDataInd Event delivered to Local SCCP User	30 min
RxSCCPUserNoticeMsgs	UDTS/XUDTS received and NNotice-Ind sent to Local SCCP User	30 min
RxSCMGMMsgs	All ingress SCMG messages (Includes, SST, SSP, SSA, MTP-Status, MTP-Pause, SS-Status)	30 min
SCCPStackQueuePeak	SCCP Stack Event Queue Peak Utilization	30 min
SCCPStackQueueAvg	SCCP Stack Event Queue Average Utilization	30 min
TxSCCPLargeMsgs	Number of large egress user data messages for segmentation	30 min
TxSCCPSegmentsPerMsg	Number of segments created for each large egress user data message	30 min
TxSCCPSegmentSUCC	Number of times segmentation procedure completed successfully	30 min
RxSCCPsgmntXudtMsgs	Number of ingress segmented XUDT messages received from network	30 min

Measurement Tag	Description	Collection Interval
RxSCCPReassSUCC	Number of times reassembly procedure completed successfully	30 min
RxSCCPSgmntReassPerMsg	Number of segments reassembled to create one large ingress user data message [Arrayed - Bucketed]	30 min
RxSCCPRtGtFrwdAppl	Number of Rt On Gt Messages forwarded to Local Application	30 min
RxSCCPRtGtXudtSgmnt	Number of Rt on Gt segmented XUDT messages received from network	30 min
RxSCCPRtSsnXudtSgmnt	Number of Rt on Ssn segmented XUDT messages received from network	30 min
RxSCCPSegmentSrvcMsg	Number of Segmented XUDTS messages received from network	30 min
RxSCCPSgmntsReassSUCC	Number of XUDT segments reassembled successfully	30 min

TxSCCPLargeMsgs

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single
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
Measurement Dimension	Single
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
Peg Condition	For each message sent to M3RL
Measurement Scope	NE, Server
Recovery	No action required.

TxSCCPSegmentsPerMsg

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Arrayed-Bucketed (Index on number of segments created for each larger egress user data message)
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	<ol style="list-style-type: none"> 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
Measurement Dimension	Single
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
Measurement Dimension	Single
Description	Egress messages sent by SCCP User to SCCP to M3RL (SCCPUser-> SCCP N-UnitDataReq->M3RL MTP-TRANSFER request)
Collection Interval	30 min
Peg Condition	For each message sent to M3RL
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
Measurement Dimension	Single
Description	The number of valid egress SCMG messages.
Collection Interval	30 min
Peg Condition	For each valid message generated by SCMG
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 GUI Main Menu: **SS7/SIGTRAN > Maintenance > Local SCCP Users** or **SS7/SIGTRAN > Maintenance > Remote MTP3 Users**.

RxSCCPMsgs

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single
Description	Ingress messages received by SCCP from M3RL (M3RL> SCCP MTP TRANSFER indication).

Collection Interval	30 min
Peg Condition	For each message received from M3RL
Measurement Scope	NE, Server
Recovery	No action required.

RxSCCPReassSUCC

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single
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
Measurement Dimension	Single
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

Measurement Dimension	Single
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.

RxSCCP Rt Ssn Xudt Sgmnt

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single
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.

RxSCCP Segment Srvc Msg

Measurement Group	Server SCCP Performance
Measurement Type	Single
Measurement Dimension	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.

RxSCCPSgmtReassPerMsg

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Arrayed-Bucketed (Index on number of segments reassembled)
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.

RxSCCPSgmntsReassSUCC

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single
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.

RxSCCPSgmtXudtMsgs

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single

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
Measurement Dimension	Single
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
Peg Condition	For each UDT/XUDT message received for SCCP user and was delivered to SCCP user.
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
Measurement Dimension	Single
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
Peg Condition	For each UDTS/XUDTS message received for SCCP user and a notification was delivered to SCCP user

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**.

RxSCMGMsgs

Measurement Group	Server SCCP Performance
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of valid ingress SCMG messages.
Collection Interval	30 min
Peg Condition	For each valid message received for SCMG
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 GUI Main Menu **SS7/SIGTRAN > Maintenance > Local SCCP Users** or **SS7/SIGTRAN > Maintenance > Remote MTP3 Users**.

SCCPStackQueuePeak

Measurement Group	Server SCCP Performance
Measurement Type	Max
Measurement Dimension	Single
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
Measurement Dimension	Single
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.

Throttling measurements

Table 43: Throttling Measurements

Measurement Tag	Measurement Description	Collection Interval
ThrottleAllow	The number of times a message was allowed	5 min
ThrottleDiscard	The number of messages that were discarded as a result of matching a rule with no response	5 min
ThrottleDiscardByName	The number of messages that were discarded as a	5 min

Measurement Tag	Measurement Description	Collection Interval
	result of matching a specific rule, by name	
ThrottleDiscardTCAP	The number of times a TCAP error was returned in conjunction with a discard	5 min
ThrottleDiscardUDTS	The number of times a UDTS was returned in conjunction with a discard	5 min
ThrottleMatch	The number of messages that matched a rule	5 min
ThrottleMatchByName	The number of messages that matched a specific rule, by name	5 min
ThrottleSimulation	The number of times a message matched a rule in the Simulation mode but was not acted upon	5 min
ThrottleWhitelistHit	The number of times a message matched a rule with Whitelist enabled, and the subscriber was in the Dn/Imsi Whitelist	5 min
ThrottleWhitelistMiss	The number of times a message matched a rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist	5 min

ThrottleAllow

Measurement Group:	Throttling
Measurement Type:	Simple
Measurement Dimension:	Single
Description:	The number of times a message was allowed (for any reason)
Collection Interval:	5 min
Peg Condition:	Each time a new incoming message was allowed to reach the HLR (for any reason)
Measurement Scope:	Network, NE, Server
Recovery:	

No action required

ThrottleDiscard

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of messages that were discarded as a result of a throttling rule
Collection Interval	5 min
Peg Condition	Each time a new incoming message matches the criteria found in Rules table and shall be throttled accordingly.
Measurement Scope	Network, NE, Server
Recovery	
No action required	

ThrottleDiscardByName

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Arrayed
Description	The number of messages that were discarded as a result of a specific throttling rule
Collection Interval	5 min
Peg Condition	Each time when a new incoming message was discarded as a result of a specific throttling rule, by name
Measurement Scope	Network, NE, Server
Recovery	
No action required	

ThrottleDiscardTCAP

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of times a TCAP error was returned in conjunction with a discard
Collection Interval	5 min

Peg Condition	Each time a TCAP error was returned in conjunction with a discard
Measurement Scope	Network, NE, Server
Recovery	No action required

ThrottleDiscardUDTS

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of times a UDTS was returned in conjunction with a discard
Collection Interval	5 min
Peg Condition	Each time a UDTS was returned in conjunction with a discard
Measurement Scope	Network, NE, Server
Recovery	No action required

ThrottleMatch

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of messages that matched a throttling rule
Collection Interval	5 min
Peg Condition	Each time a new incoming message matches a throttling rule
Measurement Scope	Network, NE, Server
Recovery	No action required

ThrottleMatchByName

Measurement Group	Throttling
Measurement Type	Simple

Measurement Dimension	Arrayed
Description	The number of messages that matched a specific throttling rule, by name
Collection Interval	5 min
Peg Condition	Each time a new incoming message matches the specific throttling rule, by name
Measurement Scope	Network, NE, Server
Recovery	No action required

ThrottleSimulation

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of times a message matched a rule but was not acted upon because the rule was in Simulation mode
Collection Interval	5 min
Peg Condition	Each time a new incoming message matches a rule but was not acted upon because the rule was in mode
Measurement Scope	Network, NE, Server
Recovery	No action required

ThrottleWhitelistHit

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of times a message matches a throttling rule with Whitelist enabled, and the subscriber is in the Dn/Imsi Whitelist
Collection Interval	5 min
Peg Condition	Each time a new incoming message matches the throttling rule with Whitelist enabled, and the subscriber is in the Dn/Imsi Whitelist
Measurement Scope	Network, NE, Server
Recovery	

No action required

ThrottleWhitelistMiss

Measurement Group	Throttling
Measurement Type	Simple
Measurement Dimension	Single
Description	The number of times a message matched a rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist
Collection Interval	5 min
Peg Condition	Each time when a new incoming message matches the throttling rule with Whitelist enabled, and the subscriber was not in the Dn/Imsi Whitelist
Measurement Scope	Network, NE, Server
Recovery	
No action required	

Transport Exception measurements

The Transport Exception measurement group contains measurements that provide information about exceptions and unexpected events related to the Transport Manager.

Measurement Tag	Description	Collection Interval
RxTrFarEndClose	Number of times the far-end closed the association	30 min
EvTrManClose	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.	30 min
EvTrNoRespClose	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.	30 min
EvTrCnxFail	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.	30 min

Measurement Tag	Description	Collection Interval
TxTrSendFail	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.	30 min
RxTrRcvFailed	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.	30 min
EvTrSockInitFail	Number of times the socket initialization failed	30 min
TmSingleTransQueueFull	The number of egress messages that were discarded because the singleTransport Writer Queue was full.	30 min
EvSctpAdjIPToDwn	Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.	30 min
EvSctpTransRej	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.	30 min

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 out 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 a lack of response (refer to the *DSR Alarms and KPIs Reference* for details about this event).
 - 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 measurements 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 (refer to the *DSR Alarms and KPIs Reference* for details about this alarm).
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 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.
3. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

EvSctpAdjPToDwn

Measurement Group	Transport Exception
Measurement Type	Max
Measurement Dimension	Arrayed (per Transport)
Description	The number of times a configured IP Address of an Adjacent Node goes from Available to Unavailable.

Collection Interval	30 min
Peg Condition	Each time reachability 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

1. If all is well, this measurement should have a zero value. A non-zero value indicates a path fault to that address was detected.
2. Otherwise:
 1. Check the event history log at **Main Menu > Alarms & Events > View History**, looking for Event 19409 - Message Rejected by ACL Filtering which provide more details as to the actual cause of the failure.
 2. Verify 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**.
 3. Verify the IP network connectivity between the MP server and the Adjacent Node's IP address using a ping or traceroute command
3. Contact [My Oracle Support \(MOS\)](#) for assistance if needed.

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.
2. 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.
3. 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.

Measurement Tag	Description	Collection Interval
EvTrCnxSuccess	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.	30 min
TmTrEnaNotUp	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.	30 min
RxTmSctpBufAvg	The Average Value of the number of bytes in SCTP RX Window.	5 min
RxTmSctpBufPeak	The Peak Value of the number of bytes in SCTP RX Window	5 min

EvTrCnxSuccess

Measurement Group	Transport Usage
Measurement Type	Simple
Measurement Dimension	Arrayed (per Transport)
Description	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 > Maintenance > 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**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.

Measurement Tag	Description	Collection Interval
TxTrOctets	The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min
RxTrOctets	The number of octets received on the SCTP/UDP Transport. It does not include SCTP, IP, or Ethernet headers.	30 min
TmSingleTransQueuePeak	The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval	30 min
TmSingleTransQueueAvg	The average single Transport Writer Queue utilization (0-100%) measured during the collection interval	30 min
SctpTransPeerCWNDPeak	The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval.	30 min
SctpTransPeerCWNDAvg	The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.	30 min
SctpTransPeerSRTTPeak	The peak value of smoothed round trip time for the SCTP Transport address during the collection interval.	30 min
SctpTransPeerSRTTAvg	The average value of smoothed round trip time for the SCTP Transport address during the collection interval.	30 min
SctpTransUnAckedDataPeak	The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.	30 min
SctpTransUnAckedDataAvg	The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.	30 min

Measurement Tag	Description	Collection Interval
SctpTransRTOPeak	The peak value of retransmission timeout in use for the SCTP Transport address	30 min
SctpTransRTOAvg	The average value of retransmission timeout in use for the SCTP Transport address	30 min

TxTrOctets

Measurement Group	Transport Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (by 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 (by 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 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 sent over the association during the reporting interval.

TmSingleTransQueuePeak

Measurement Group	Transport Performance
Measurement Type	Max
Measurement Dimension	Arrayed (by 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 needed 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.
 - a) 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.
 - b) 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**.
 - c) 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**.
 - d) 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.
 - e) 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 (by Transport)
Description	The average single Transport (SCTP/UDP) 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 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**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).

SctpTransUnAkedDataPeak

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).

SctpTransUnAkedDataAvg

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 average value of retransmission timeout in use for the Sctp Transport address

Collection Interval 30

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).

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).

A

ACK	Data Acknowledgement
ANSI	<p>American National Standards Institute</p> <p>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.</p>
ASP	<p>Application Server Process</p> <p>A process instance of an Application Server. An Application Server Process serves as an active or standby process of an Application Server (for example, 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, and may be configured to process signaling traffic within more than one Application Server.</p>
Association	<p>An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.</p>

B

B

BIOS	Basic Input-Output System Firmware on the CPU blade that is executed prior to executing an OS.
------	---

C

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.
------	---

CMOS	Complementary Metal Oxide Semiconductor CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.
------	--

ComAgent	Communication Agent A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.
----------	--

Communication Agent	See ComAgent.
---------------------	---------------

CPC	Capability Point Code
-----	-----------------------

C

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).

D

DAVA

Destination Available

DB

Database

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

DP

Data Processor

The repository of subscriber data on the individual node elements. The DP hosts the full address resolution database.

DRST

Destination Restricted

DUNA

Destination Unavailable

DUPU

Destination User Part Unavailable

D

An M3UA management message.

F

FABR

Full Address Based Resolution

Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.

FIPS

Federal Information Processing Standard

Full Address Based Resolution

See FABR.

G

GT

Global Title Routing Indicator

GTI

Global Title Indicator

GUI

Graphical User Interface

The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA

High Availability

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

H

HIDS Host Intrusion Detection System

HP Hewlett-Packard

I

IP 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.

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.

K

KPI Key Performance Indicator

L

LSP Local Signaling Point

A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique

L

primary/true point code within a particular SS7 Domain to an MP server.

M

M3RL

M3UA Routing Layer

A layer invented by Tekelec to enhance M3UA by adding a true routing layer.

M3UA

SS7 MTP3-User Adaptation Layer

M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.

MP

Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

MPS

Messages Per Second

A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.

MTP3

Message Transfer Part, Level 3

N

NI

Network Indicator

N

NOAM	Network Operations, Administration, and Maintenance
NTP	Network Time Protocol
NTP daemon	Network Time Protocol daemon – NTP process that runs in the background.

O

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.
OPC	Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.

P

PDBI	Provisioning Database Interface The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDDBA.
PDU	Protocol Data Unit

P

Perl
An object-oriented, event-driven programming language.

R

RBAR
Range Based Address Resolution
A DSR enhanced routing application which allows you to route Diameter end-to-end transactions based on Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges.

RI
Routing Indicator

RSP
Remote Signaling Point
A logical element that represents a unique point code within a particular SS7 domain with which the SS7 application's Local Signaling Point interacts.

S

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

S

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.

SG

Signaling Gateway

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 (for example, 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.

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network

S

management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

SOAM	System Operations, Administration, and Maintenance
SOAP	Simple Object Access Protocol
SS7	Signaling System #7 A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.
STP	Signal Transfer Point The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.
SW	Switch

T

T

TFA	TransFer Allowed (Msg)
TFC	Transfer Control
TFP	TransFer Prohibited (Msg) A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.
TFR	Transfer Restricted
TPC	True Point Code

X

XUDT	Extended User Data
------	--------------------