Oracle® Communications
Diameter Signaling Router

Subscriber Database Server Alarms, KPIs, and Measurements

Reference

E73331 Revision 02

March 2017

Oracle Communications Diameter Signaling Router Subscriber Database Server Alarms, KPIs, and

Measurements Reference

Table of Contents

Chapter 1: Introduction....................21

Overview....................22

Scope and Audience....................22

Manual Organization....................22

Documentation Admonishments....................23

Related Specifications....................23

Locate Product Documentation on the Oracle Help Center Site....................23

Customer Training....................24

My Oracle Support (MOS)....................24

Emergency Response....................25

Chapter 2: User Interface Introduction....................26

User interface organization....................27

User Interface Elements....................27

Main menu options....................28

Missing Main Menu options....................29

Common Graphical User Interface Widgets....................29

System Login Page....................30

Main Menu Icons....................31

Work Area Displays....................32

Customizing the Splash Page Welcome Message....................35

Column headers (sorting)....................35

Page Controls....................35

Optional Layout Element Toolbar....................36

Filters....................37

Auto refresh controls....................39

Pause Updates....................40

Max Records Per Page Controls....................40

Message display....................40

Chapter 3: Alarms and Events, KPIs, and Measurements Overview....................41

Alarms Warning....42
Viewing the file list....42
Data Export....42
Data Export elements....42
Configuring data export....44
Tasks....45
Active Tasks....45
Scheduled Tasks....48

Chapter 4: Alarms and Events....51
General alarms and events information....52
Alarms and events overview....52
Alarm and event ID ranges....53
Alarm and event types....54
Viewing active alarms....56
Active alarms data export elements....56
Exporting active alarms....57
Generating a report of active alarms....58
Viewing alarm and event history....59
Historical events data export elements....59
Exporting alarm and event history....60
Generating a report of historical alarms and events....61
OAM (10000-10999)....62
Alarms formatting information....62
10000 - Incompatible database version....62
10001 - Database backup started....63
10002 - Database backup completed....63
10003 - Database backup failed....63
10004 - Database restoration started....64
10005 - Database restoration completed....64
10006 - Database restoration failed....64
10008 - Database provisioning manually disabled 65
10009 - Config and Prov db not yet synchronized 65
10010 - Stateful db from mate not yet synchronized....65
10011 - Cannot monitor table....66
10012 - Table change responder failed 66
10115 - Health Check Started....66
10116 - Health Check Successful....67
10117 - Health Check Failed....67
10118 - Health Check Not Run....67

10020 - Backup failure 68
10050 - Resource Audit Failure....................68
10051 - Route Deployment Failed....................68
10052 - Route discovery failed....................69
10053 - Route deployment failed - no available device....................69
10054 - Device deployment failed....................69
10055 - Device discovery failed....................70
10073 - Server Group Max Allowed HA Role Warning....................70
10074 - Standby server degraded while mate server stabilizes....................70
10075 - Application processes have been manually stopped....................71
10078 - Application not restarted on standby server due to disabled failure cleanup mode....................71
10100 - Log export started....................72
10101 - Log export successful....................72
10102 - Log export failed....................72
10103 - Log export already in progress....................73
10104 - Log export file transfer failed....................73
10105 - Log export cancelled - user request....................73
10106 - Log export cancelled - duplicate request....................74
10107 - Log export cancelled - queue full....................74
10108 - Duplicate scheduled log export task....................75
10109 - Log export queue is full....................75
10134 - Server Upgrade Failed....................76
10151 - Login successful....................77
10152 - Login failed....................77
10153 - Logout successful....................78
10154 - User Account Disabled....................78
10155 - SAML Login Successful....................78
10156 - SAML Login Failed....................79
10200 - Remote database reinitialization in progress....................79
SDS (14000-14999)....................80
Alarms formatting information....................80
14100 - Interface Disabled....................80
14101 - No Remote Connections....................80
14102 - Connection Failed....................81
14103 - Both Port Identical....................81
14120 - Connection Established....................81
14121 - Connection Terminated....................82
14122 - Connection Denied....................82
14140 - Import Throttled....................82
14150 - Import Initialization Failed....................83

14151 - Import Generation Failed....83
14152 - Import Transfer Failed....84
14153 - Export Initialization Failed....84
14154 - Export Generation Failed....84
14155 - Export Transfer Failed....85
14160 - Import Operation Completed....85
14161 - Export Operation Completed....85
14170 - Remote Audit started and in progress....86
14171 - Remote Audit aborted....86
14172 - Remote Audit failed to complete....86
14173 - Remote Audit completed....87
14174 - NPA Split pending request deleted....87
14175 - NPA Split activation failed....87
14176 - NPA Split started and is active....88
14177 - NPA Split completion failed....88
14178 - NPA Split completed....88
14179 - MSISDN deleted from Blacklist....89
14180 - IMSI deleted from Blacklist....89
14188 - PdbRelay not connected....89
14189 - PdbRelay Time Lag....90
14198 - ProvDbException....90
14200 - DP Stack Event Queue utilization....91
14301- ERA Responder Failed....91
Communication Agent, ComAgent (19800-19899)....91
19800 - Communication Agent Connection Down....92
19801 - Communication Agent Connection Locally Blocked....92
19802 - Communication Agent Connection Remotely Blocked....93
19803 - Communication Agent stack event queue utilization....94
19804 - Communication Agent configured connection waiting for remote client to establish connection....95
19805 - Communication Agent Failed To Align Connection....96
19806 - Communication Agent CommMessage mempool utilization....97
19807 - Communication Agent User Data FIFO Queue utilization....98
19808 - Communication Agent Connection FIFO Queue utilization....98
19810 - Communication Agent Egress Message Discarded....99
19811 - Communication Agent Ingress Message Discarded....100
19814 - Communication Agent Peer has not responded to heartbeat....101
19816 - Communication Agent Connection State Changed....101
19817 - Communication Agent DB Responder detected a change in configurable control option parameter....101
19820 - Communication Agent Routed Service Unavailable....102

19821 - Communication Agent Routed Service Degraded...103
19822 - Communication Agent Routed Service Congested...103
19823 - Communication Agent Routed Service Using Low-Priority Connection Group...104
19824 - Communication Agent Pending Transaction Utilization...104
19825 - Communication Agent Transaction Failure Rate...105
19826 - Communication Agent Connection Congested...106
19827 - SMS stack event queue utilization...106
19830 - Communication Agent Service Registration State Change...107
19831 - Communication Agent Service Operational State Changed...107
19832 - Communication Agent Reliable Transaction Failed...107
19833 - Communication Agent Service Egress Message Discarded...108
19842 - Communication Agent Resource-Provider Registered...109
19843 - Communication Agent Resource-Provider Resource State Changed...109
19844 - Communication Agent Resource-Provider Stale Status Received...109
19845 - Communication Agent Resource-Provider Deregistered...110
19846 - Communication Agent Resource Degraded...110
19847 - Communication Agent Resource Unavailable...110
19848 - Communication Agent Resource Error...111
19850 - Communication Agent Resource-User Registered...111
19851 - Communication Agent Resource-User Deregistered...112
19852 - Communication Agent Resource Routing State Changed...112
19853 - Communication Agent Resource Egress Message Discarded...112
19854 - Communication Agent Resource-Provider Tracking Table Audit Results...113
19855 - Communication Agent Resource Has Multiple Actives...113
19856 - Communication Agent Service Provider Registration State Changed...114
19857 - Communication Agent Service Provider Operational State Changed...114
19858 - Communication Agent Connection Rejected...115
19860 - Communication Agent Configuration Daemon Table Monitoring Failure...115
19861 - Communication Agent Configuration Daemon Script Failure...116
19862 - Communication Agent Ingress Stack Event Rate...116
19863 - Communication Agent Max Connections Limit In Connection Group Reached...117
19864 - ComAgent Successfully Set Host Server Hardware Profile...117
19865 - ComAgent Failed to Set Host Server Hardware Profile...118
19866 - Communication Agent Peer Group Status Changed...118
19867 - Communication Agent Peer Group Egress Message Discarded...118
19868 - Communication Agent Connection Rejected - Incompatible Network...119
EXG Stack (19000-19999)...119
19420 - BDFQFull...119
19421 - BDFThrotl...120

19422 - BDFInvalidPkt....120
19900 - DP Server CPU utilization....121
19901 - CFG-DB Validation Error....121
19902 - CFG-DB Update Failure....121
19903 - CFG-DB post-update Error....122
19904 - CFG-DB post-update Failure....122
19905 - Measurement Initialization Failure....123
Platform (31000-32800)....123
31000 - S/W fault....123
31001 - S/W status....124
31002 - Process watchdog failure....124
31003 - Tab thread watchdog failure....124
31100 - Database replication fault....125
31101 - Database replication to slave failure....125
31102 - Database replication from master failure....125
31103 - DB Replication update fault....126
31104 - DB Replication latency over threshold....126
31105 - Database merge fault....127
31106 - Database merge to parent failure....127
31107 - Database merge from child failure....128
31108 - Database merge latency over threshold....128
31109 - Topology config error....128
31110 - Database audit fault....129
31111 - Database merge audit in progress....129
31112 - DB replication update log transfer timed out....130
31113 - DB replication manually disabled....130
31114 - DB replication over SOAP has failed....130
31115 - Database service fault....131
31116 - Excessive shared memory....131
31117 - Low disk free....132
31118 - Database disk store fault....132
31119 - Database updatelog overrun....132
31120 - Database updatelog write fault....133
31121 - Low disk free early warning....133
31122 - Excessive shared memory early warning....134
31123 - Database replication audit command complete....134
31124 - ADIC error....134
31125 - Database durability degraded....135
31126 - Audit blocked....135
31127 - DB Replication Audit Complete....136
31128 - ADIC Found Error....136

31129 - ADIC Found Minor Issue....136
31130 - Network health warning....137
31131 - DB Ousted Throttle Behind....137
31140 - Database perl fault....137
31145 - Database SQL fault....138
31146 - DB mastership fault....138
31147 - DB upsynclog overrun....139
31148 - DB lock error detected....139
31200 - Process management fault....140
31201 - Process not running....140
31202 - Unkillable zombie process....140
31206 - Process mgmt monitoring fault....141
31207 - Process resource monitoring fault....141
31208 - IP port server fault....142
31209 - Hostname lookup failed....142
31213 - Process scheduler fault....142
31214 - Scheduled process fault....143
31215 - Process resources exceeded....143
31216 - SysMetric configuration error....144
31220 - HA configuration monitor fault....144
31221 - HA alarm monitor fault....144
31222 - HA not configured....145
31223 - HA Heartbeat transmit failure....145
31224 - HA configuration error....145
31225 - HA service start failure....146
31226 - HA availability status degraded....146
31227 - HA availability status failed....147
31228 - HA standby offline....147
31229 - HA score changed....147
31230 - Recent alarm processing fault....148
31231 - Platform alarm agent fault....148
31232 - Late heartbeat warning....149
31233 - HA Path Down....149
31234 - Untrusted Time Upon Initialization 149
31235 - Untrusted Time After Initialization 150
31236 - HA Link Down....150
31240 - Measurements collection fault....151
31250 - RE port mapping fault....151
31260 - SNMP Agent....152
31270 - Logging output....152
31280 - HA Active to Standby transition....152

31281 - HA Standby to Active transition....153
31282 - HA Management Fault....153
31283 - Lost Communication with server....153
31284 - HA Remote Subscriber Heartbeat Warning....154
31285 - HA Node Join Recovery Entry....154
31286 - HA Node Join Recovery Plan....155
31287 - HA Node Join Recovery Complete....155
31290 - HA Process Status....155
31291 - HA Election Status....156
31292 - HA Policy Status....156
31293 - HA Resource Link Status....156
31294 - HA Resource Status....157
31295 - HA Action Status....157
31296 - HA Monitor Status....157
31297 - HA Resource Agent Info....158
31298 - HA Resource Agent Detail....158
31299 - HA Notification Status....158
31300 - HA Control Status....159
31301 - HA Topology Events....159
32100 - Breaker Panel Feed Unavailable....160
32101 - Breaker Panel Breaker Failure....160
32102 - Breaker Panel Monitoring Failure....160
32103 - Power Feed Unavailable....161
32104 - Power Supply 1 Failure....161
32105 - Power Supply 2 Failure....161
32106 - Power Supply 3 Failure....162
32107 - Raid Feed Unavailable....162
32108 - Raid Power 1 Failure....162
32109 - Raid Power 2 Failure....163
32110 - Raid Power 3 Failure....163
32111 - Device Failure....163
32112 - Device Interface Failure....164
32113 - Uncorrectable ECC memory error....164
32114 - SNMP get failure....164
32115 - TPD NTP Daemon Not Synchronized Failure....165
32116 - TPD Server's Time Has Gone Backwards....166
32117 - TPD NTP Offset Check Failure....166
32300 - Server fan failure....167
32301 - Server internal disk error....168
32302 - Server RAID disk error....168
32303 - Server Platform error....169

32304 - Server file system error....169
32305 - Server Platform process error....170
32306 - Server RAM shortage error....170
32307 - Server swap space shortage failure....170
32308 - Server provisioning network error....171
32309 - Eagle Network A Error....172
32310 - Eagle Network B Error....172
32311 - Sync Network Error....172
32312 - Server disk space shortage error....173
32313 - Server default route network error....174
32314 - Server temperature error....174
32315 - Server mainboard voltage error....175
32316 - Server power feed error....176
32317 - Server disk health test error....176
32318 - Server disk unavailable error....177
32319 - Device error....177
32320 - Device interface error....178
32321 - Correctable ECC memory error....178
32322 - Power Supply A error....179
32323 - Power Supply B error....179
32324 - Breaker panel feed error....180
32325 - Breaker panel breaker error....180
32326 - Breaker panel monitoring error....183
32327 - Server HA Keepalive error....184
32328 - DRBD is unavailable....184
32329 - DRBD is not replicating....185
32330 - DRBD peer problem....185
32331 - HP disk problem....186
32332 - HP Smart Array controller problem....186
32333 - HP hpacucliStatus utility problem....187
32334 - Multipath device access link problem....187
32335 - Switch link down error....188
32336 - Half Open Socket Limit....188
32337 - Flash Program Failure....189
32338 - Serial Mezzanine Unseated....189
32339 - TPD Max Number Of Running Processes Error....190
32340 - TPD NTP Daemon Not Synchronized Error....190
32341 - TPD NTP Daemon Not Synchronized Error....191
32342 - NTP Offset Check Error....192
32343 - TPD RAID disk 192
32344 - TPD RAID controller problem....193

32345 - Server Upgrade snapshot(s) invalid......193
32346 - OEM hardware management service reports an error......194
32347 - The hwmgmtcliStatus daemon needs intervention......194
32348 - FIPS Subsystem Problem 195
32349 - File Tampering......195
32500 - Server disk space shortage warning......196
32501 - Server application process error......196
32502 - Server hardware configuration error......197
32503 - Server RAM shortage warning......197
32504 - Software Configuration Error......198
32505 - Server swap space shortage warning......198
32506 - Server default router not defined......199
32507 - Server temperature warning......200
32508 - Server core file detected......200
32509 - Server NTP Daemon not synchronized......201
32510 - CMOS battery voltage low......202
32511 - Server disk self test warning......202
32512 - Device warning......203
32513 - Device interface warning......203
32514 - Server reboot watchdog initiated......203
32515 - Server HA failover inhibited......204
32516 - Server HA Active to Standby transition......204
32517 - Server HA Standby to Active transition......205
32518 - Platform Health Check failure......205
32519 - NTP Offset Check failure......205
32520 - NTP Stratum Check failure......206
32521 - SAS Presence Sensor Missing......207
32522 - SAS Drive Missing......207
32523 - DRBD failover busy......208
32524 - HP disk resync......208
32525 - Telco Fan Warning......209
32526 - Telco Temperature Warning......209
32527 - Telco Power Supply Warning......210
32528 - Invalid BIOS value......210
32529 - Server Kernel Dump File Detected......211
32530 - TPD Upgrade Failed......211
32531 - Half Open Socket Warning Limit......211
32532 - Server Upgrade Pending Accept/Reject......212
32533 - TPD Max Number Of Running Processes Warning......212
32534 - TPD NTP Source Is Bad Warning......213
32535 - TPD RAID disk resync......214

32536 - TPD Server Upgrade snapshot(s) warning....214
32537 - FIPS subsystem warning event....215
32540 - CPU Power limit mismatch....215
32700 - Telco Switch Notification....215
32701 - HIDS Initialized....216
32702 - HIDS Baseline Deleted....216
32703 - HIDS Enabled....216
32704 - HIDS Disabled....216
32705 - HIDS Monitoring Suspended....217
32706 - HIDS Monitoring Resumed....217
32707 - HIDS Baseline Updated....217

Chapter 5: Key Performance Indicators (KPIs)....218

General KPIs information....219
KPIs overview....219
KPIs....219
Viewing KPIs....219
KPIs data export elements....219
Exporting KPIs....220
KPIs server elements 221
Provisioning KPIs....222
Process-based KPIs....223
DP KPIs....224
Communication Agent (ComAgent) KPIs....225

Chapter 6: Measurements....226

General measurements information....227
Measurements....227
Measurement elements....227
Generating a measurements report....228
Measurements data export elements....229
Exporting measurements reports....230
Provisioning interface measurements....231
ProvConnectsAttempted....233
ProvConnectsAccepted....233
ProvConnectsDenied....234
ProvConnectsFailed....234
ProvConnectionIdleTimeouts....234
ProvMsgsReceived....235
ProvMsgsSuccessful....235

ProvMsgsFailed....235
ProvMsgsSent....236
ProvMsgsDiscarded....236
ProvMsgsImported....237
ProvTxnCommitted....237
ProvTxnWriteMutexTimeouts....237
ProvTxnFailed....238
ProvTxnAborted....238
ProvTxnTotal....238
ProvTxnDurabilityTimeouts....239
ProvRelayMsgsSent....239
ProvRelayMsgsSuccessful....239
ProvRelayMsgsFailed....240
ProvImportsSuccessful....240
ProvImportsFailed....240
ProvExportsSuccessful....241
ProvExportsFailed....241
ProvDnSplitCreated....241
ProvDnSplitRemoved....242
ProvNpaSplitStarted....242
ProvNpaSplitCompleted....242
ProvRemoteAuditMsgsSent....243
ProvRelayTimeLag....243
ProvDbException....243
RemoteAuditCompleted....244
RemoteAuditStarted....244
DP Measurements....244
DpsQueriesReceived....246
DpsMsisdnQueriesReceived....246
DpsImsiQueriesReceived....247
DpsNaiQueriesReceived....247
DpsQueriesFailed....247
DpsMsisdnQueriesFailed....247
DpsImsiQueriesFailed....248
DpsNaiQueriesFailed....248
DpsSuccessResponses....248
DpsMsisdnSuccessResponses....249
DpsImsiSuccessResponses....249
DpsNaiSuccessResponses....249
DpsNotFoundResponses....250
DpsMsisdnNotFoundResponses....250

DpsImsiNotFoundResponses....250
DpsNaiNotFoundResponses....251
DpsRespSent....251
DpsIngressQueuePeak....251
DpsIngressQueueAvg....252
DpsIngressQueueFull....252
DpsQueryRatePeak....252
DpsQueryRateAvg....253
DpsQueryProcessingTime....253
DpsQueryProcessingTimeAvg....253
DpsMsisdnBlacklistedResponses....254
DpsImsiBlacklistedResponses....254
DpsMsisdnPrefixFound....254
DpsImsiPrefixFound....255
DpsMsisdnBlacklistLookups....255
DpsImsiBlacklistLookups....255
DpsMsisdnPrefixLookups....256
DpsImsiPrefixLookups....256
Communication Agent (ComAgent) Performance measurements....256
CAAvgDataFIFOQueueUtil....258
CAAvgMxFIFOQueueUtil....259
CAAvgQueueUtil....260
CAAvgRsrcPoolUtil....260
CAAvgRxStackEvents....261
CAAvgTxStackEvents....261
CADSTx....261
CAHSTxRsrc....262
CAHSTxRsrcRateAvg....262
CAHSTxRsrcRateMax....263
CAPeakDataFIFOQueueUtil....263
CAPeakMxFIFOQueueUtil....263
CAPeakQueueUtil....264
CAPeakRsrcPoolUtil....264
CAPeakRxStackEvents....265
CAPeakTxStackEvents....265
CAPSTxGrp....266
CAPSTxGrpSuccess....266
CARSTx....267
CARx....267
CARxSuccess....267
CATransEndAbnorm....268

CATransEndAbnormRateAvg 268
CATransEndAbnormRateMax 269
CATransEndNorm....................269
CATransPendingAvg 270
CATransPendingMax 270
CATransRateAvg 271
CATransRateMax 271
CATransStarted 271
CATransTimeAvg 272
CATransTimeMax 272
CATx....................272
CATxSuccess....................273
Communication Agent (ComAgent) Exception measurements....................274
CADataFIFOQueueFul....................277
CADSTxDscrdCong 278
CAHSRsrcErr....................279
CAHSTxDscrdIntErrSR....................279
CAHSTxDscrdCongSR....................280
CAHSTxDscrdIntErrSR....................280
CAHSTxDscrdUnavailSR....................281
CAHSTxDscrdUnknownSR....................281
CAHSTxDscrdUnkwnRsrc....................282
CAHSTxRsrc....................282
CAMxFIFOQueueFul....................283
CAPSTxDscrdUnkwnGrp....................283
CAPSTxDscrdUnavailGrp....................284
CAPSTxDscrdCongPeer....................284
CARsrcPoolFul 285
CARSTxDscrdCong 285
CARSTxDscrdInternalErr....................286
CARSTxDscrdSvcUnavail 286
CARxDiscUnexpEvent 287
CARxDscrdBundle....................287
CARxDscrdConnUnavail....................288
CARxDscrdDecodeFailed 288
CARxDscrdIncompat 288
CARxDscrdInternalErr 289
CARxDscrdLayerSendFail 289
CARxDscrdMsgLenErr 290
CARxDscrdUnkServer 290
CARxDscrdUnkStkLyr 291

CARxMsgUnknown 291
CAStackQueueFul 292
CATransDscrdInvCorrId 292
CATransDscrdStaleErrRsp 293
CATransEndAbnorm 293
CATransEndAbnormRateAvg 294
CATransEndAbnormRateMax 294
CATransEndAnsErr 295
CATransEndErr 295
CATransEndNoResources..296
CATransEndNoResponse..296
CATransEndUnkwnSvc..297
CATransEndUnregSvc 297
CATransNoReTxMaxTTL..298
CATransRetx 298
CATransReTxExceeded..299
CATransStaleSuccessRsp 299
CATransTTLExceeded..300
CATxDscrdBundle..300
CATxDscrdConnUnAvail..301
CATxDscrdDestUserIncmpat..301
CATxDscrdEncodeFail..302
CATxDscrdInternalErr 302
CATxDscrdMxSendFail..303
CATxDscrdUnknownSvc 303
CATxDscrdUnkServer 303
CATxDscrdUnregSvc 304
OAM.ALARM measurements..304
OAM.SYSTEM measurements..305

Glossary..307

List of Figures

Figure 1: Oracle System Login....30

Figure 2: Paginated Table....32

Figure 3: Scrollable Table....33

Figure 4: Form Page....33

Figure 5: Tabbed Pages....34

Figure 6: Tabbed Pages....34

Figure 7: Report Output....34

Figure 8: Sortable and Non-sortable Column Headers....35

Figure 9: Optional Layout Element Toolbar....36

Figure 10: Automatic Error Notification....37

Figure 11: Examples of Filter Styles....38

Figure 12: Flow of Alarms....52

Figure 13: Alarm Indicators Legend....53

Figure 14: Trap Count Indicator Legend....53

Figure 15: Breaker Panel LEDs....181

Figure 16: Breaker Panel Setting....182

List of Tables

Table 1: Admonishments....23

Table 2: User Interface Elements....27

Table 3: SDS Main Menu User Interface Options....28

Table 4: Main Menu Icons....31

Table 5: Example Action Buttons....35

Table 6: Submit Buttons....36

Table 7: Filter Control Elements....38

Table 8: Data Export Elements....42

Table 9: Active Tasks Elements....45

Table 10: Active Tasks Report Elements....48

Table 11: Scheduled Tasks Elements....49

Table 12: Alarm/Event ID Ranges....53

Table 13: Alarm and Event Types....54

Table 14: Schedule Active Alarm Data Export Elements....56

Table 15: Schedule Event Data Export Elements....59

Table 16: Schedule KPI Data Export Elements....220

Table 17: KPIs Server Elements....221

Table 18: Provisioning KPIs....222

Table 19: Process-based KPIs....223

Table 20: DP KPIs....224

Table 21: Communication Agent KPIs....225

Table 22: Measurements Elements....228

Table 23: Schedule Measurement Data Export Elements.....229

Table 24: Application Routing Rule Measurements.....231

Table 25: DP Measurements.....244

Table 26: Communication Agent Performance Measurement Report Fields.....256

Table 27: Communication Agent Exception Measurement Report Fields.....274

Table 28: OAM Alarm Measurements.....304

Table 29: OAM System Measurements.....305

Chapter 1

Introduction

Topics:

- *Overview.....22*
- *Scope and Audience.....22*
- *Manual Organization.....22*
- *Documentation Admonishments.....23*
- *Related Specifications.....23*
- *Locate Product Documentation on the Oracle Help Center Site.....23*
- *Customer Training.....24*
- *My Oracle Support (MOS).....24*
- *Emergency Response.....25*

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 *SDS Alarms, KPIs, and Measurements* documentation provides information about SDS alarms and events, 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 SDS feature. The manual provides preventive and corrective procedures that will aid personnel in maintaining the SDS.

The corrective maintenance procedures are those used in response to a system alarm or output message. These procedures are used to aid in the detection, isolation, and repair of faults.

Manual Organization

Information in this document is organized into the following sections:

- *Introduction* contains general information about this document, how to contact *My Oracle Support (MOS)*, and *Locate Product Documentation on the Oracle Help Center Site*.
- *User Interface Introduction* describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.
- *Alarms and Events, KPIs, and Measurements Overview* provides general information about the application's alarms and events, KPIs, and measurements.
- *Alarms and Events* provides information and recovery procedures for alarms and events, organized first by alarm category, then numerically by the number that appears in the application.
- *Key Performance Indicators (KPIs)* provides detailed KPI information, organized alphabetically by KPI name.

- *Measurements* provides detailed measurement information, organized alphabetically by measurement category.

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 *personal injury*.)
WARNING	Warning: (This icon and text indicate the possibility of *equipment damage*.)
CAUTION	Caution: (This icon and text indicate the possibility of *service interruption*.)
TOPPLE	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Specifications

For information about additional publications related to this document, refer to the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at *http://docs.oracle.com*.

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

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

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

User Interface Introduction

Topics:

- *User interface organization.....27*
- *Missing Main Menu options.....29*
- *Common Graphical User Interface Widgets.....29*

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

User interface organization

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

User Interface Elements

Table 2: User Interface Elements describes elements of the user interface.

Table 2: User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	The left side of the banner provides the following information: • Displays the company name, • product name and version, and • the alarm panel. The right side of the banner: • Allows you to pause any software updates. • Links to the online help for all software. • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different

Element	Location	Function
		elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Login Message*.
Session Banner	Across the bottom of the web page	The left side of the banner provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner shows the alarm panel.

Main menu options

The menu options that appear on the screen differ according to whether you are logged into an SDS or DP SOAM. *Table 3: SDS Main Menu User Interface Options* describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options would not appear on the screen of a user who does not have administrative privileges.

Table 3: SDS Main Menu User Interface Options

Menu Item	Function
Administration	The Administration menu allows you to: • Set up and manage user accounts • Configure group permissions • View session information • Authorize IP addresses to access the user interface • Configure options including, but not limited to, password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Configure SNMP services

Menu Item	Function
	• Validate and transfer ISO files • Prepare, initiate, monitor, and complete upgrades • View the software versions report
Configuration	Provides access to configuring network elements, servers, server groups, and systems.
Alarms & Events	Lists active alarms and alarm history.
Security Log	Allows you to view and export security log data.
Status & Manage	Allows you to monitor the statuses of server processes, both collectively and individually, as well as perform actions required for server maintenance. Also allows you to view the status of file management systems, and to manage data files on servers throughout the system.
Measurements	Allows you to view, modify, import, and export measurement data.
Communication Agent	Provides infrastructure features and services for enabling inter-server communication.
SDS	Provides maintenance and configuration options related to SDS.
Help	Launches the online help system for the user interface.
Logout	Allows you to log out of the user interface.

Missing Main Menu options

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

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

Common Graphical User Interface Widgets

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

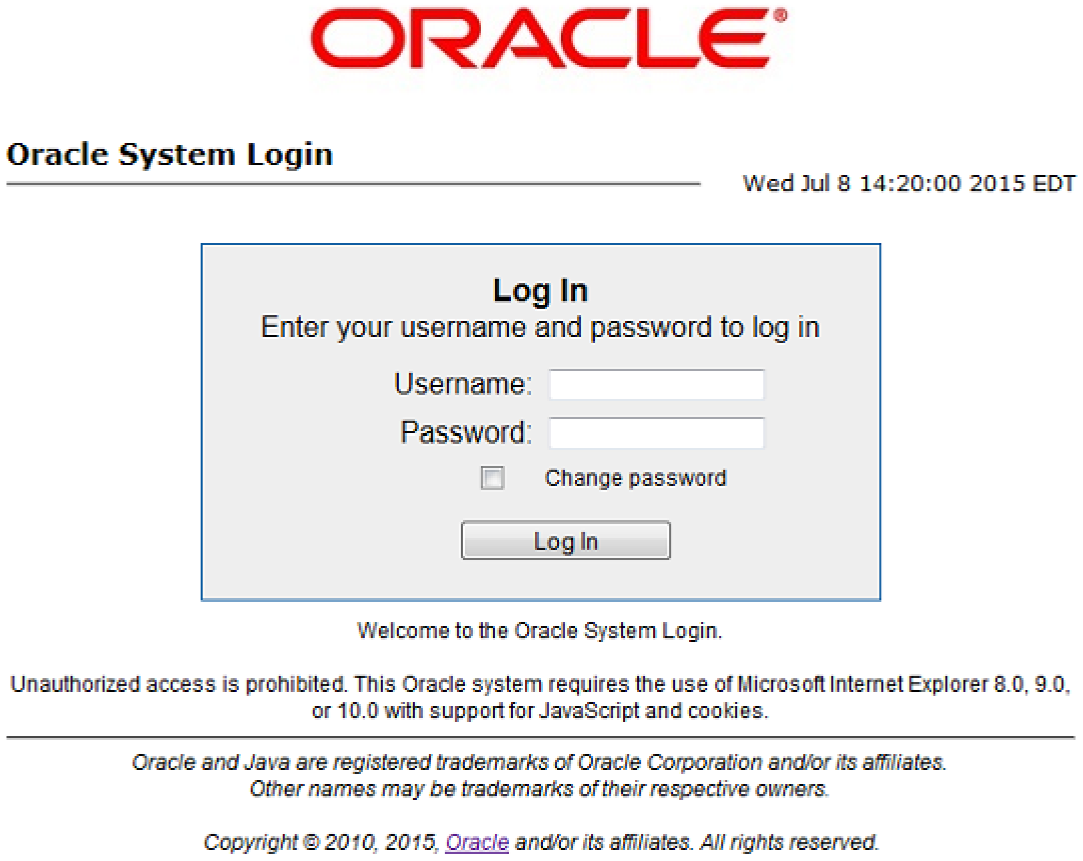
System Login Page

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

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

Customizing the Login Message

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



Oracle System Login

Wed Jul 8 14:20:00 2015 EDT

Log In

Enter your username and password to log in

Username:

Password:

□ Change password

Welcome to the Oracle System Login.

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

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

Copyright © 2010, 2015, Oracle and/or its affiliates. All rights reserved.

Figure 1: Oracle System Login

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

   The **General Options Administration** page appears.

2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.

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

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

Supported Browsers

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

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

Main Menu Icons

This table describes the icons used in the **Main Menu**.

Table 4: Main Menu Icons

Icon	Name	Description
⊞ 📁	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.
🗒	Config File	Contains operations in an Options page.
🔍	File with Magnifying Glass	Contains operations in a Status View page.
📄	File	Contains operations in a Data View page.
🗐	Multiple Files	Contains operations in a File View page.
❓	File with Question Mark	Contains operations in a Query page.
👤	User	Contains operations related to users.

Icon	Name	Description
👥	Group	Contains operations related to groups.
✓	Task	Contains operations related to Tasks
?	Help	Launches the Online Help.
Zz	Logout	Logs the user out of the user interface.

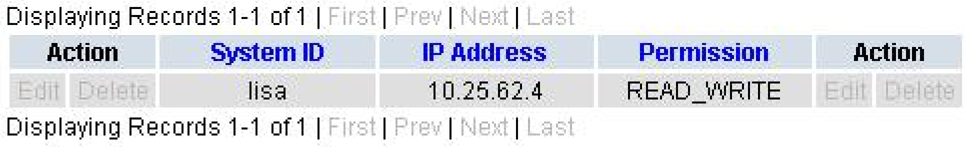
Work Area Displays

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

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

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see *Page Controls*.



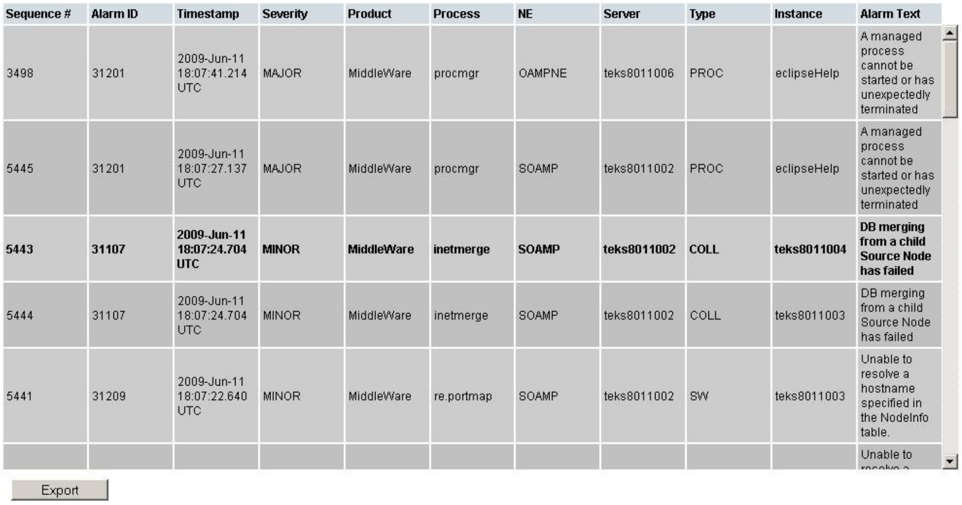
Displaying Records 1-1 of 1 | First | Prev | Next | Last

Action	System ID	IP Address	Permission	Action
Edit Delete	lisa	10.25.62.4	READ_WRITE	Edit Delete

Displaying Records 1-1 of 1 | First | Prev | Next | Last

Figure 2: Paginated Table

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



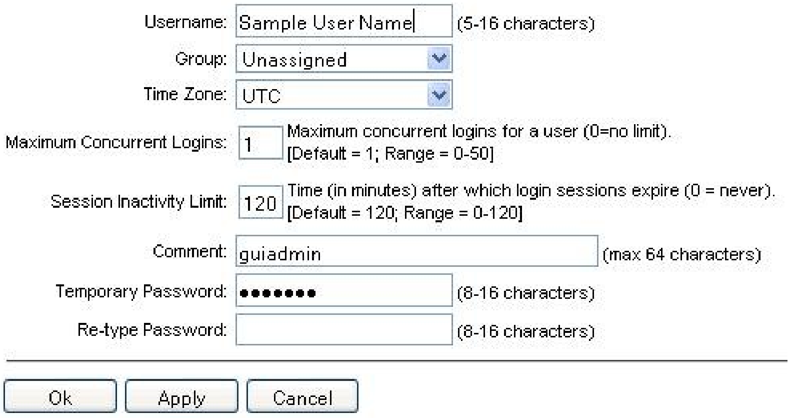
Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR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

Figure 3: Scrollable Table

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

Forms

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

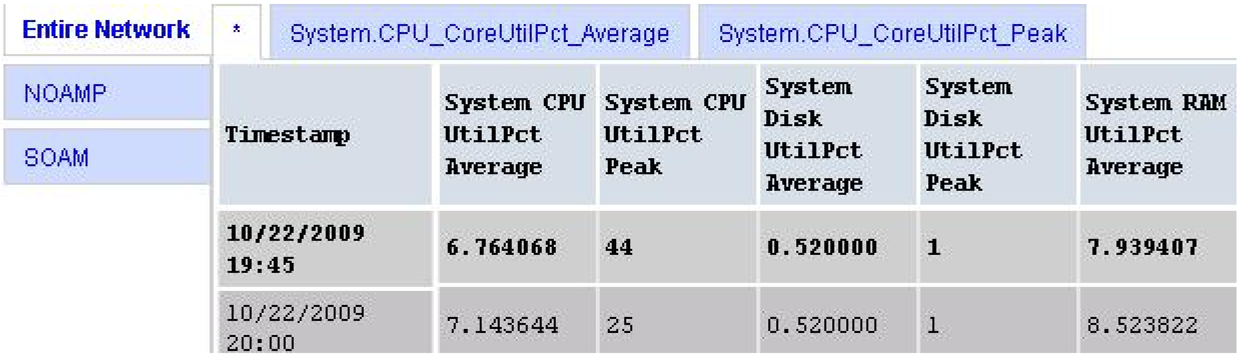


Username:	Sample User Name	(5-16 characters)
Group:	Unassigned	
Time Zone:	UTC	
Maximum Concurrent Logins:	1	Maximum concurrent logins for a user (0=no limit). [Default = 1; Range = 0-50]
Session Inactivity Limit:	120	Time (in minutes) after which login sessions expire (0 = never). [Default = 120; Range = 0-120]
Comment:	guiadmin	(max 64 characters)
Temporary Password:	•••••••	(8-16 characters)
Re-type Password:		(8-16 characters)

Figure 4: Form Page

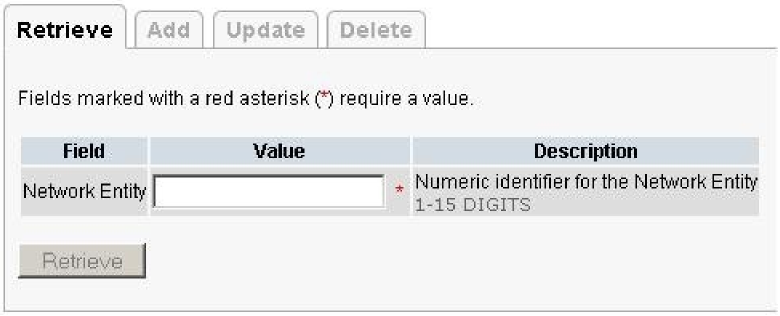
Tabbed pages

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



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

Figure 5: Tabbed Pages



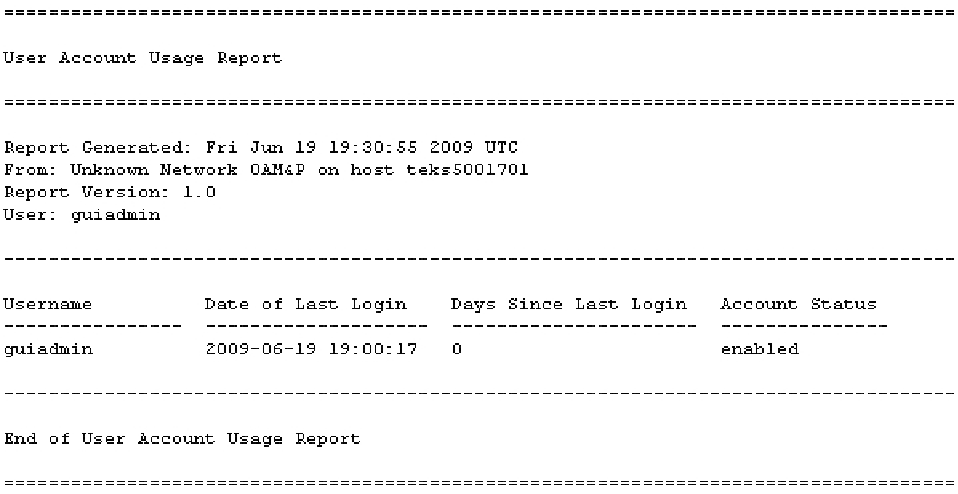
Fields marked with a red asterisk (*) require a value.

Field	Value	Description
Network Entity	*	Numeric identifier for the Network Entity 1-15 DIGITS

Figure 6: Tabbed Pages

Reports

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



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

User Account Usage Report

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

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

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

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

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

End of User Account Usage Report

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

Figure 7: Report Output

Customizing the Splash Page Welcome Message

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

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Locate **Welcome Message** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.
   A status message appears at the top of the page to inform you if the operation was successful.

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

Column headers (sorting)

Some column headers are links that, when clicked, sort the table by that column. Sorting does not affect filtering. Column headers that are black and group column headers are not sortable.

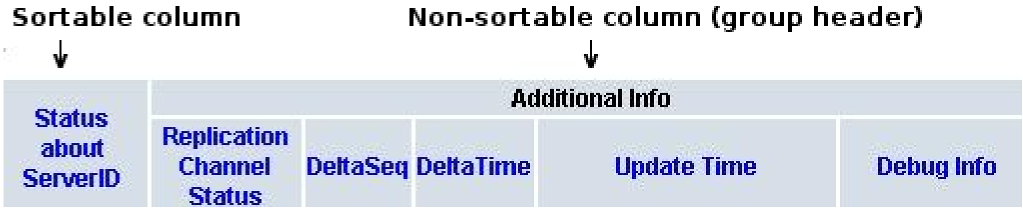


Figure 8: Sortable and Non-sortable Column Headers

Page Controls

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

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

Table 5: Example Action Buttons contains examples of Action buttons.

Table 5: Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.

Action Button	Function
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in *Table 6: Submit Buttons*, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The Submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 6: Submit Buttons

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

Optional Layout Element Toolbar

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

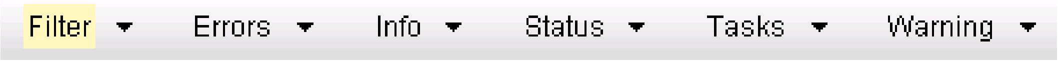


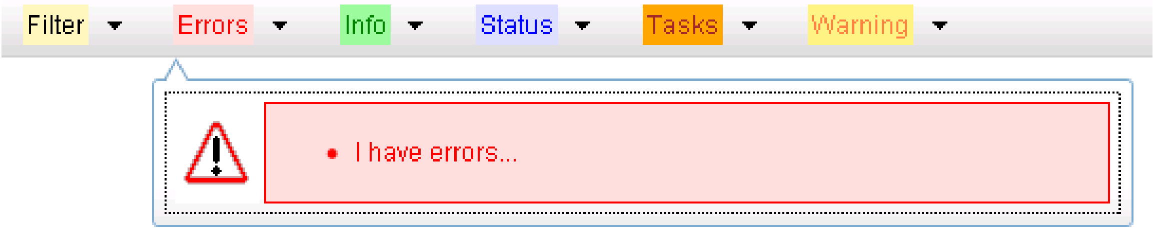
Figure 9: Optional Layout Element Toolbar

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

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

Notifications

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



- I have errors...

Figure 10: Automatic Error Notification

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

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

Opening an Element in the Toolbar

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

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

   The selected element opens and overlays the work area.

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

Filters

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

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

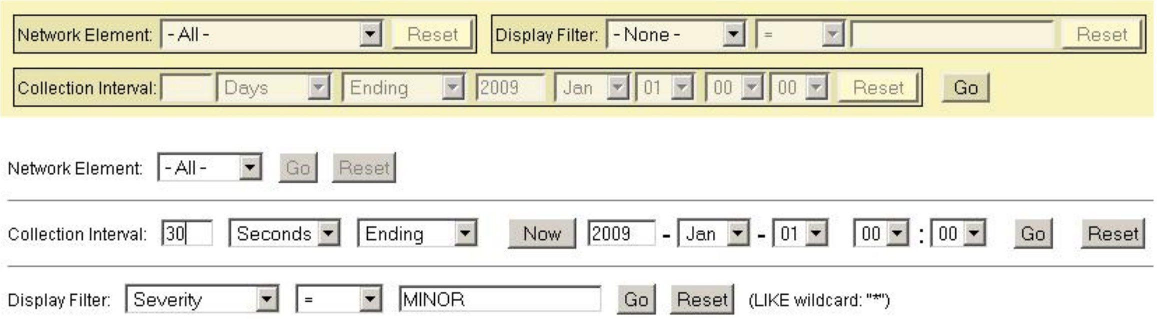
- Network Element – When enabled, the Network Element filter limits the data viewed to a single Network Element.

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

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

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

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



Network Element: - All -

Display Filter: - None - =

Collection Interval: Days Ending 2009 Jan 01 00 00

Network Element: - All -

Collection Interval: 30 Seconds Ending 2009 - Jan - 01 00 : 00

Display Filter: Severity = MINOR (LIKE wildcard: "*")

Figure 11: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter Control Elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

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

Filtering on the Network Element

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

1. Click **Filter** in the optional layout element toolbar.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

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

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

   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.

   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering Using the Display Filter

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

1. Click **Filter** in the optional layout element toolbar.
2. Select a field name from the **Display Filter** pulldown menu.

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

   The selected field name displays in the **Display Filter** field.
3. Select an operator from the operation selector pulldown menu.
4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.
5. For data tables that support compound filtering, click **Add** to add another filter condition. Then repeat steps 2 through 4.

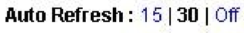
   Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Auto refresh controls

Auto refresh controls are widgets that control the rate at which the Page Area refreshes on some pages. They are located in the Page Control Area on the right side. Auto refresh can be set to **15** seconds or **30** seconds, and it can be turned off. The changes take effect immediately.

Click one of the Auto Refresh options to set the auto refresh rate. Click the **Off** option to terminate automatic refreshing of the page.



Auto Refresh : 15 | 30 | Off

Pause Updates

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

Max Records Per Page Controls

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

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

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

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

   OK saves the change and returns to the previous page.

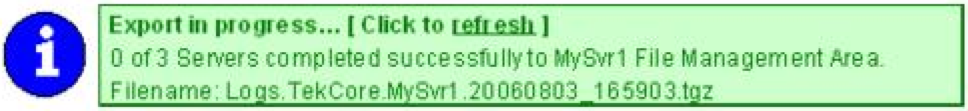
   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

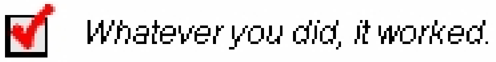
Message display

A message appears at the top of the Work Area on a page when a process needs to communicate errors or information. When an event is in progress, a refresh link may be provided here so that you can refresh without having to use the browser's refresh function

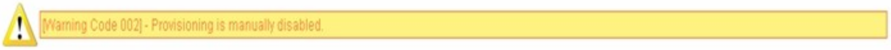
These are examples of some of the messages that can appear in a Work Area:



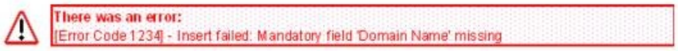
Export in progress... [Click to refresh]
0 of 3 Servers completed successfully to MySvr1 File Management Area.
Filename: Logs.TekCore.MySvr1.20060803_165903.tgz



Whatever you did, it worked.



[Warning Code 002] - Provisioning is manually disabled.



There was an error:
[Error Code 1234] - Insert failed: Mandatory field 'Domain Name' missing

Chapter 3

Alarms and Events, KPIs, and Measurements Overview

Topics:

- *Alarms Warning.....42*
- *Viewing the file list.....42*
- *Data Export.....42*
- *Tasks.....45*

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

Alarms Warning

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

Viewing the file list

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

1. From the Main menu, select **Status & Manage** > **Files**.
2. Select a server.
   All files stored on the selected server are displayed.

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 8: Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server	Must be a valid hostname or a valid IP address. Range: Maximum length is 255 characters; alphanumeric characters (a-z, A-Z, and 0-9) and minus sign. Hostname must start and end with an alphanumeric.

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

Element	Description	Data Input Notes
		Default: 12:00 AM
Day of Week	If Upload Frequency is Weekly, this is the day of the week when exported data files will be transferred to the export server	Format: Radio button Range: Sunday through Saturday Default: Sunday
SSH Key Exchange	This button initiates an SSH key exchange between the OAM server and the data export server currently defined on the page. A password must be entered before the exchange can complete.	Format: Button
Transfer Now	This button initiates an immediate attempt to transfer any data files in the export directory to the export server	Format: Button
Test Transfer	This button initiates an immediate test transfer to the data export server currently defined on the page.	Format: Button
Keys Report	This button generates an SSH Keys Report for all OAM servers.	Format: Button

Configuring data export

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

1. Select **Administration** > **Remote Servers** > **Data Export**.
2. Enter a **Hostname**.
   See *Data Export elements* for details about the **Hostname** field and other fields that appear on this page.
3. Enter a **Username**.
4. Enter a **Directory Path** on the Export server.
5. (Optional) Enter the **Path to Rsync** on the Export server.

   Note: Depending on the OS and implementation of the remote server, it may be required to define the path to the rsync binary on the export server but this is not common. If no path is specified, the username's home directory on the export server is used.
6. Select whether to enable the transfer of the backup file. To leave the backup disabled, do not check the box.

7. Select the **File Compression** type.
8. Select the **Upload Frequency**.
9. If you selected hourly for the upload frequency, select the **Minute** intervals.
10. If you selected daily or weekly for the upload frequency, select the **Time of Day**.
11. If you selected weekly for the upload frequency, select the **Day of the Week**.
12. If public keys were manually placed on the Export server, skip to step *Step 14*. Otherwise, click **Exchange SSH Key** to transfer the SSH keys to the Export server.
13. Enter the password.
    The server attempts to exchange keys with the export server currently defined on the page. After the SSH keys are successfully exchanged, continue with the next step.
14. Click **OK** to apply the changes or **Cancel** to discard the changes.
    The export server is now configured and available to receive performance and configuration data.
15. You may optionally click **Test Transfer** to confirm the ability to export to the server currently defined on the page.
    The user can monitor the progress of the task by selecting the **Tasks** drop down list in the page control area.

Tasks

The **Tasks** pages display the active, long running tasks and scheduled tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results for long running tasks, while the **Scheduled Task**s 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 9: Active Tasks Elements

Active Tasks Element	Description
ID	Task ID
Name	Task name

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

Deleting a task

Use this procedure to delete one or more tasks.

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

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

   All active tasks on the selected server are displayed.
3. Select one or more tasks.

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

   Note: You can select multiple rows to delete at one time. To select multiple rows, press and hold Ctrl as you click to select specific rows.
4. Click **Delete**.
5. Click **OK** to delete the selected task(s).

Deleting all completed tasks

Use this procedure to delete all completed tasks.

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

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

   All active tasks on the selected server are displayed.
3. Click **Delete all Completed**.
4. Click **OK** to delete all completed tasks.

Cancelling a running or paused task

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

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

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

   All active tasks on the selected server are displayed.
3. Select a task.
4. Click **Cancel**.
5. Click **OK** to cancel the selected task.

Pausing a task

Use this procedure to pause a task.

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

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

   All active tasks on the selected server are displayed.
3. Select a task.

   Note: A task may be paused only if the status of the task is running.
4. Click **Pause**.
   A confirmation box appears.
5. Click **OK** to pause the selected task.
   For information about restarting a paused task, see *Restarting a task*.

Restarting a task

Use this procedure to restart a task.

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

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

   All active tasks on the selected server are displayed.
3. Select a paused task.

   Note: A task may be restarted only if the status of the task is paused.
4. Click **Restart**.
   A confirmation box appears.
5. Click **OK** to restart the selected task.
   The selected task is restarted.

Active Tasks report elements

The **Active Tasks [Report]** page displays report data for selected tasks. This table describes elements on the **Active Tasks [Report]** page.

Table 10: Active Tasks Report Elements

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

Generating an active task report

Use this procedure to generate an active task report.

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

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

   All active tasks on the selected server are displayed.
3. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria is included in the report.
4. Click **Report**.
5. Click **Print** to print the report.
6. Click **Save** to save the report.

Scheduled Tasks

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

- *Exporting active alarms*
- *Exporting alarm and event history*
- *Exporting KPIs*
- *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 11: Scheduled Tasks Elements

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

Editing a scheduled task

Use this procedure to edit a scheduled task.

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

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

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

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

   All scheduled tasks are displayed on the **Scheduled Tasks** page.
2. Select one or more tasks.
3. Click **Delete**.
4. Click **OK** to delete the selected task(s).

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

1. Select **Status & Manage** > **Tasks** > **Scheduled Tasks**.
   All scheduled tasks are displayed on the **Scheduled Tasks** page.
2. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria is included in the report.
3. Click **Report**.
4. Click **Print** to print the report.
5. Click **Save** to save the report.

Chapter 4

Alarms and Events

Topics:

- *General alarms and events information.....52*
- *OAM (10000-10999).....62*
- *SDS (14000-14999).....80*
- *Communication Agent, ComAgent (19800-19899).....91*
- *EXG Stack (19000-19999).....119*
- *Platform (31000-32800).....123*

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

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

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

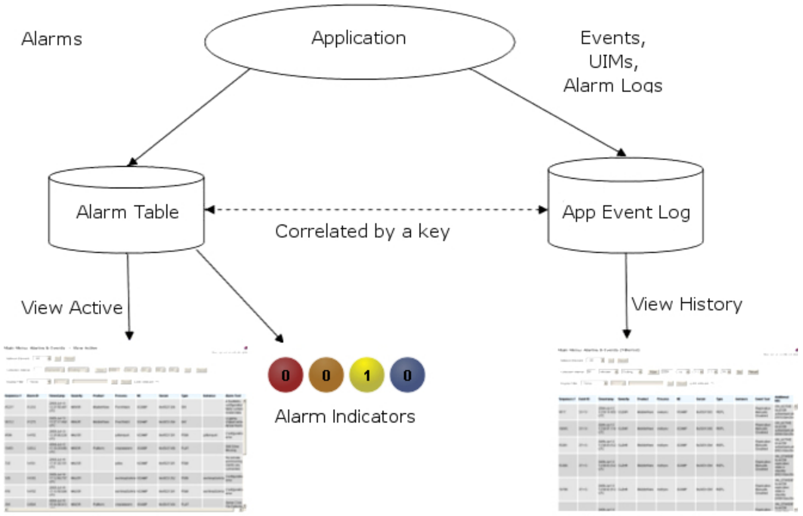
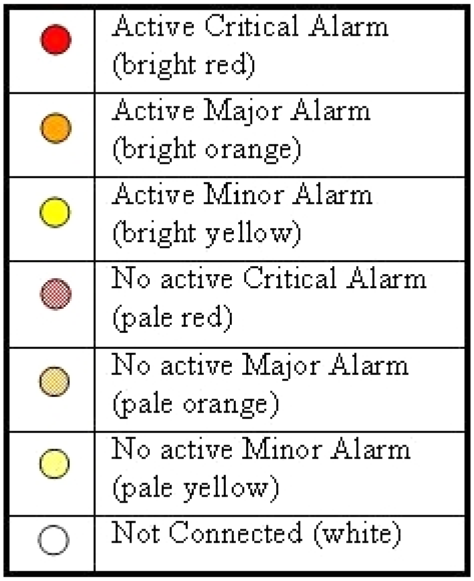


Figure 12: Flow of Alarms

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:

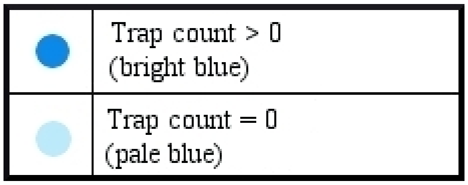
- Record events that represent alarmed conditions
- Record events for later browsing
- Implement an event interface for generating SNMP traps

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 13: Alarm Indicators Legend



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

Figure 14: Trap Count Indicator Legend

Alarm and event ID ranges

The **Alarm ID** listed for each alarm falls into one of the following process classifications:

Table 12: Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5099
OAM	10000-10999

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

Alarm and event types

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

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

Table 13: 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

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

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

Viewing active alarms

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

Use this procedure to view active alarms.

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

1. Select **Alarms & Events** > **View Active**.
2. If necessary, specify filter criteria and click **Go**.
   The active alarms are displayed according to the specified criteria.

   The active alarms table updates automatically. When new alarms are generated, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

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

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

Active alarms data export elements

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

Table 14: 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: Option Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data is written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting active alarms

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

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered 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**.

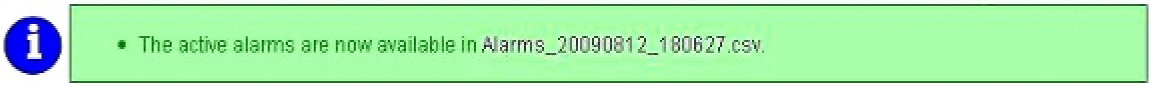
   Note: **Day of Week** is not an option if **Export Frequency** equals **Once**.

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 *Viewing the file list*.

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

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

9. Click **Export**.
   The file is exported.
10. Click the link in the green message box to go directly to the **Status & Manage** > **Files** page.



- The active alarms are now available in Alarms_20090812_180627.csv.

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

Generating a report of active alarms

Use this procedure to generate a report.

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

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

3. Click **Report**.
   The View Active Report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Viewing alarm and event history

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

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

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

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

   Historical alarms and events are displayed according to the specified criteria.

   The historical alarms table updates automatically. When new historical data is available, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

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

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

Historical events data export elements

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

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

Exporting alarm and event history

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

During data export, the system automatically creates a CSV file of the filtered data. The file 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**.

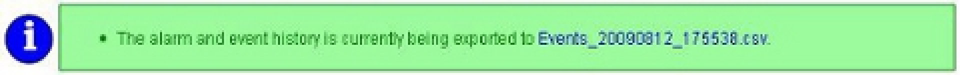
   Note: Day of Week is not an option if **Export Frequency** equals **Once**.

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 *Viewing the file list*.

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

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

10. Click **Export**.
    The file is exported.
11. Click the link in the green message box to go directly to the **Status & Manage** > **Files** page.



- The alarm and event history is currently being exported to Events_20090812_175538.csv.

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**.
2. Specify filter criteria, if necessary, and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Report**.
   The View History Report can be printed or saved to a file.
4. Click **Print** to print the report.

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

OAM (10000-10999)

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

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

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:

It is recommended to contact *My Oracle Support (MOS)*.

10001 - Database backup started

Event Type:	DB
Description:	The database backup has started.
Severity:	Info
Instance:	GUI
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecBackupStartNotify

Recovery:

No action action required.

10002 - Database backup completed

Event Type:	DB
Description:	Backup completed
Severity:	Info
Instance:	GUI
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecBackupCompleteNotify

Recovery:

No action required.

10003 - Database backup failed

Event Type:	DB
Description:	The database backup has failed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecBackupFailNotify

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

10004 - Database restoration started

Event Type:	DB
Description:	The database restoration has started.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecRestoreStartNotify

Recovery:

No action required.

10005 - Database restoration completed

Event Type:	DB
Description:	The database restoration is completed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecRestoreCompleteNotify

Recovery:

No action required.

10006 - Database restoration failed

Event Type:	DB
Description:	The database restoration has failed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	1
OID:	tekelecRestoreFailNotify

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

10008 - Database provisioning manually disabled

Alarm Group:	DB
Description:	Database provisioning has been manually disabled.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	This alarm does not autoclear.
OID:	awpss7TekelecProvisioningManuallyDisabledNotify

Recovery:

No action required.

10009 - Config and Prov db not yet synchronized

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

Recovery:

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

10010 - Stateful db from mate not yet synchronized

Alarm Group:	HA
Description:	The stateful database is not synchronized with the mate database.
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, it is recommended to 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:

It is recommended to 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:

It is recommended to contact *My Oracle Support (MOS)*.

10115 - Health Check Started

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

Recovery:

No action required.

10116 - Health Check Successful

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

Recovery:

No action required.

10117 - Health Check Failed

Event Type:	LOG
Description:	Upgrade health check operation failed.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	N/A
OID:	tekelecLogHealthCheckFailed

Recovery:

No action required.

10118 - Health Check Not Run

Event Type:	LOG
Description:	Upgrade health check not run.
Severity:	Info
Instance:	N/A
HA Score:	Normal
Throttle Seconds:	N/A
OID:	tekelecLogHealthCheckNotRun

Recovery:

It is recommended to 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. It is recommended to 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, it is recommended to 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, it is recommended to 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:	Normal
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:

It is recommended to contact *My Oracle Support (MOS)*.

10100 - Log export started

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

Recovery:

No action required.

10101 - Log export successful

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

Recovery:

No action required.

10102 - Log export failed

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

Recovery:

1. Verify the export request and try the export again.

2. If the problem persists, it is recommended to 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:

It is recommended to 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:

It is recommended to 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, it is recommended to 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, it is recommended to 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:

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

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:

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

10134 - Server Upgrade Failed

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

Recovery:

1. If a server upgrade fails, this alarm clears when the server upgrades successfully. Upgrade the server individually or as part of a server group or site upgrade. If more than one server in the same server group or site fails to upgrade, the server group and site upgrades may be useful because both methods will attempt to upgrade all of the failed servers within the server group or site, respectively. Upgrading all servers in a server group is useful if the server group has multiple upgrade failures. Upgrading all servers in a site is useful if servers in multiple server groups contained in a site have upgrade failures.
2. To upgrade individual servers:
   a) Navigate to the Upgrade page (**Administration** > **Software Management** > **Upgrade**).
   b) To upgrade a NOAM server, select the NOAM tab and proceed to *Substep e*.
   c) To upgrade a server that is not a NOAM server, select the SOAM site tab associated with the server(s) that raised the alarm.
   d) Select the sub-tab associated with the server group containing the server(s) that raised the alarm.
   e) Select the individual server(s) and then click the **Upgrade Server** button to start the upgrade on the selected servers.

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

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

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

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

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

   a) Navigate to the Upgrade page (**Administration** > **Software Management** > **Upgrade**).

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

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

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

4. To upgrade entire sites:

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

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

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

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 it is recommended to 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, it is recommended to contact *My Oracle Support (MOS)*.

SDS (14000-14999)

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

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 *General alarms and events information*.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm (Critical, Major, Minor, Informational)
- Instance: where the alarm occurred, for example, GUI, <process name>, IP address, <server name>

  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 must pass before the alarm will clear itself. Some alarms are not autocleared. Informational events are marked N/A because they do not have to be cleared.
- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

14100 - Interface Disabled

Alarm Type: PROV

Description: Provisioning interface is manually disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

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

OID: sdsProvInterfaceDisabled

Recovery: Enable the interface to clear the alarm.

14101 - No Remote Connections

Alarm Group	PROV
Description	No remote provisioning clients are connected.
Severity	Major

Instance	N/A
HA Score	Normal
Auto Clear Seconds	This alarm does not automatically clear.
OID	sdsProvNoRemoteConnections

Recovery

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

14102 - Connection Failed

Alarm Group	PROV
Description	Provisioning client connection initialization failed due to an error specified in additional information. See trace log for details. (CID=<Connection ID>, IP=<IP Address>).
Severity	Major
Instance	N/A
HA Score	Normal
Auto Clear Seconds	300
OID	sdsProvConnectionFailed

Recovery

Alarm automatically clears after 5 minutes or when connected.

14103 - Both Port Identical

Alarm Group	PROV
Description	Both XML and SOAP provisioning client connection are disables since same port is configured for both.
Severity	Major
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID	sdsProvBothPortIdentical

Recovery

Alarm clears when one of the ports is changed.

14120 - Connection Established

Event Type	PROV
Description	Provisioning client connection established.

Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvConnectionEstablished

Recovery

No action required for this event.

14121 - Connection Terminated

Event Type	PROV
Description	Provisioning client connection terminated due to the error specified in additional information.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvConnectionTerminated

Recovery

No action required for this event.

14122 - Connection Denied

Event Type	PROV
Description	Provisioning client connection denied due to the error specified in additional information.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvConnectionDenied

Recovery

No action required for this event.

14140 - Import Throttled

Alarm Group	PROV

Description	Provisioning import throttled to prevent overrunning database service processes.
Severity	Minor
Instance	N/A
HA Score	Normal
Auto Clear Seconds	5
OID	sdsProvImportThrottled

Recovery

Alarm automatically cleared in 5 seconds after throttling subsides.

14150 - Import Initialization Failed

Alarm Group	PROV
Description	Provisioning import failed due to the initialization error specified in additional information. See trace log for details.
Severity	Major
Instance	provimport
HA Score	Normal
Auto Clear Seconds	N/A
OID	sdsProvImportInitializationFailed

Recovery

Alarm clears when initialization completes successfully.

14151 - Import Generation Failed

Alarm Group	PROV
Description	Provisioning import failed due to the import file execution error specified in the additional information. See the trace log for details.
Severity	Major
Instance	provimport
HA Score	Normal
Auto Clear Seconds	12 hours
OID	sdsProvImportGenerationFailed

Recovery

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

14152 - Import Transfer Failed

Alarm Group	PROV
Description	Provisioning import operation failed due to the file transfer error specified in additional information. See trace log for details.
Severity	Major
Instance	provimport
HA Score	Normal
Auto Clear Seconds	12 hours
OID	sdsProvImportTransferFailed

Recovery

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

14153 - Export Initialization Failed

Alarm Group	PROV
Description	Provisioning export failed due to the initialization error specified in the additional information. See trace log for details.
Severity	Major
Instance	provexport
HA Score	Normal
Auto Clear Seconds	12 hours
OID	sdsProvExportInitializationFailed

Recovery

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

14154 - Export Generation Failed

Alarm Group	PROV
Description	Provisioning export operation failed due to the export file generation error specified in the additional information. See trace log for details.
Severity	Major
Instance	provexport
HA Score	Normal
Auto Clear Seconds	12 hours

OID	sdsProvExportGenerationFailed

Recovery

Correct the problem and try the export again.

14155 - Export Transfer Failed

Alarm Group	PROV
Description	Provisioning export operation failed due to the file transfer error specified in the additional information. See trace log for details.
Severity	Major
Instance	provexport
HA Score	Normal
Auto Clear Seconds	12 hours
OID	sdsProvExportTransferFailed

Recovery

Correct the problem and try the export again.

14160 - Import Operation Completed

Event Type	PROV
Description	All files were imported successfully.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvImportOperationCompleted

Recovery

No action required for this event.

14161 - Export Operation Completed

Event Type	PROV
Description	All scheduled exports completed successfully.
Severity	Info
Instance	N/A
HA Score	Normal

Throttle Seconds	N/A
OID	sdsProvExportOperationCompleted

Recovery

No action required for this event.

14170 - Remote Audit started and in progress

Event Type	PROV
Description	Remote Audit started and is in progress.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvRemoteAuditStartedAndInProgressNotify

Recovery

No action required for this event.

14171 - Remote Audit aborted

Event Type	PROV
Description	Remote Audit aborted.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvRemoteAuditAbortedNotify

Recovery

No action required for this event.

14172 - Remote Audit failed to complete

Event Type	PROV
Description	Remote Audit failed to complete.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A

OID	sdsProvRemoteAuditFailedToCompleteNotify

Recovery

No action required for this event.

14173 - Remote Audit completed

Event Type	PROV
Description	Remote Audit completed successfully.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvRemoteAuditCompletedNotify

Recovery

No action required for this event.

14174 - NPA Split pending request deleted

Event Type	PROV
Description	A Pending NPA Split has been deleted by the user before it could become Active on its Start Date.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvNpaSplitPendingRequestDeleted

Recovery

No action required for this event.

14175 - NPA Split activation failed

Event Type	PROV
Description	NPA Split activation failed. See trace log for details.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A

OID	sdsProvNpaSplitActivationFailed

Recovery

Contact the *My Oracle Support (MOS)*.

14176 - NPA Split started and is active

Event Type	PROV
Description	NPA Split started and is active.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvNpaSplitActivated

Recovery

No action required for this event.

14177 - NPA Split completion failed

Event Type	PROV
Description	NPA Split completion failed. See trace log for details.
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	N/A
OID	sdsProvNpaSplitCompletionFailed

Recovery

Contact the *My Oracle Support (MOS)*.

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.

14179 - MSISDN deleted from Blacklist

Event Type	PROV
Description	Previously Blacklisted MSISDN is now a Routing Entity
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	0
OID	sdsProvMsisdnDeletedFromBlacklist

Recovery

No action necessary.

14180 - IMSI deleted from Blacklist

Event Type	PROV
Description	Previously Blacklisted IMSI is now a Routing Entity
Severity	Info
Instance	N/A
HA Score	Normal
Throttle Seconds	0
OID	sdsProvImsiDeletedFromBlacklist

Recovery

No action necessary.

14188 - PdbRelay not connected

Alarm Group	PROV
Description	PdbRelay not connected. • The SDS Command Log does not go back far enough to resume relaying commands. A bulk load of HLRR is required. • Neither Primary nor Disaster Recovery Virtual IP address is configured for the HLRR. • The connection is failing with the error shown in Additional Info.
Severity	Major
Instance	pdbrelay

HA Score	Normal
Auto Clear Seconds	0
OID	sdsProvRelayNotConnectedNotify

Recovery

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

14189 - PdbRelay Time Lag

Alarm Group	PROV
Description	Pdbrelay feature is enabled but is falling behind. The time between timestamps of the last record processed and the latest entry in the Command Log has exceeded time limit threshold. • Critical: 27 minutes • Major - 12 minutes • Minor - 3 minutes
Severity	Critical, Major, Minor
Instance	pdbrelay
HA Score	Normal
Auto Clear Seconds	0
OID	sdsProvRelayTimeLagNotify

Recovery

Contact the *My Oracle Support (MOS)*.

14198 - ProvDbException

Alarm Group	PROV
Description	The rate of ProvDbException errors has exceed the threshold. • Critical - 1000 errors per second • Major - 100 errors per second • Minor - Any occurrence
Severity	Critical, Major, Minor
Instance	ProvDbException, SDS
HA Score	Normal
Auto Clear Seconds	3600
OID	sdsProvDbExceptionNotify

Recovery

No action required.

14200 - DP Stack Event Queue utilization

Alarm Group	DPS
Description	The percent utilization of the DP Stack Event Queue is approaching its maximum capacity.
Severity	• Minor when utilization exceeds 60%. • Major when utilization exceeds 80%. • Critical when utilization exceeds 95%.
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID	sdsDpsStackEventQueueUtilizationNotify

Recovery

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

14301- ERA Responder Failed

Alarm Group	ERA
Description	Event responder failed due to an internal error.
Severity	Major
Instance	N/A
HA Score	Normal
Auto Clear Seconds	N/A
OID	sdsEraResponderFailed

Recovery

Contact the *My Oracle Support (MOS)*.

Communication Agent, ComAgent (19800-19899)

This section provides information and recovery procedures for Communication Agent (ComAgent) alarms and events, ranging from 19800 - 19899, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

19800 - Communication Agent Connection Down

Alarm 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. It is recommended to contact *My Oracle Support (MOS)* for assistance.

19801 - Communication Agent Connection Locally Blocked

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

and so this alarm may indicate that applications are unable to communicate with their expected set of peers.

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

Severity: Minor

Instance: N/A

Note: This alarm is cleared when:

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnLocalBlockedNotify

Recovery:

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

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

19802 - Communication Agent Connection Remotely Blocked

Alarm Group: CAF

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

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

Severity:	Minor
Instance:	N/A

Note: This alarm is cleared when:

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

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

Recovery:

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

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

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

19803 - Communication Agent stack event queue utilization

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. It is recommended to contact *My Oracle Support (MOS)* for assistance.

2. Use **Main Menu** > **Status & Control** > **KPIs** to monitor the ingress traffic rate of each MP.

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

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

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

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

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

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

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

HA Score: Normal

Auto Clear Seconds: 300 (5 min)

OID:	cAFClientConnWaitNotify

Recovery:

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

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

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

19806 - Communication Agent CommMessage mempool utilization

Alarm Group:	CAF
Description:	The percent utilization of the Communication Agent CommMessage mempool is approaching defined threshold capacity. The percent utilization of the Communication Agent internal resource pool (CommMessage) is approaching its defined capacity. If this problem persists and the usage reaches 100% utilization, ComAgent will allocate the CommMessage objects from the heap. This should not impact the functionality, but may impact performance and/or latency.
Severity:	Critical, Major, Minor
Instance:	<ComAgent Process Name>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFPoolResUtilNotify

Recovery:

1. Use **Main Menu** > **Alarms & Events** to examine the alarm log.

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

2. Use **Main Menu** > **Status & Control** > **KPIs** to monitor the ingress traffic rate of each MP.

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

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

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

19807 - Communication Agent User Data FIFO Queue utilization

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.

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

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

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

4. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Main Menu** > **Status & Control** > **KPIs**.

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

19808 - Communication Agent Connection FIFO Queue utilization

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.

   It is recommended to contact *My Oracle Support (MOS)* for assistance.
3. The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from **Main Menu** > **Status & Control** > **KPIs**.

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.
4. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Main Menu** > **Status & Control** > **KPIs**.

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

   It is recommended to contact *My Oracle Support (MOS)* for assistance.

19810 - Communication Agent Egress Message Discarded

Event Type:	CAF
Description:	The Communication Agent egress message is being discarded due to one of the following reasons: • Unknown destination server • Connection state is not InService • Incompatible destination • Serialization failed • MxEndpoint send failed • Internal error

Severity:	Info
Instance:	<RemoteIP> **Note:** If <RemoteIP> is not known at the time of message discard, then "Unknown" will be used.
HA Score:	Normal
Throttle Seconds:	10
OID:	cAFEventEgressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

   Message is being discarded due to one of the reasons specified.

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

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

Event Type:	CAF
Description:	Communication Agent DB Responder detected a change in configurable control option parameter. **Note:** This event is an indication that Communication Agent detected a control parameter change. The change will be applied to applicable software

	component. If the change is applied on the GUI, the appropriate GUI action is logged in security logs. If the action is not performed from GUI and the control parameter is changed, this event indicates the executed change.
Severity:	Info
Instance:	N/A
HA Score:	Normal
OID:	cAFEventComAgtConfigParamChangeNotify

Recovery:

1. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
2. Use **Main Menu** > **Security Log** and examine the alarm log.
3. If the event shows up in **Main Menu** > **Alarms & Events**, without the corresponding GUI security-log in **Main Menu** > **Security Log**. It is recommended to contact *My Oracle Support (MOS)* for assistance.

19820 - Communication Agent Routed Service Unavailable

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

Recovery:

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

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

19821 - Communication Agent Routed Service Degraded

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

Recovery:

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

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

19822 - Communication Agent Routed Service Congested

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

Recovery:

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

2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the are congested and the degree to which they are congested.
3. Check the far-end of the congested connections in order to further isolate the cause of congestion.

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

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

Alarm Group:	CAF
Description:	Communication Agent routed service is routing traffic using a connection group that has a lower-priority than another connection group.
Severity:	Major
Instance:	<ServiceName>
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	cAFRSUsingLowPriConnGrpNotify

Recovery:

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

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.
4. It is recommended to contact *My Oracle Support (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. It is recommended to 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. It is recommended to 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 overload by traffic from other MPs.
   b) The local server may be trying to send too much traffic to the remote.
   c) The IP connectivity may be impaired.
6. It is recommended to contact *My Oracle Support (MOS)* for assistance.

19827 - SMS stack event queue utilization

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

OID:	cAFSmsQueueUtilNotify

Recovery:

1. The system itself may be heavily loaded with work, causing this subsystem to also become overloaded. Check other system resources (ComAgent Congestion, Cpu Utilization, and Server Congestion are some examples) for signs of overload.
2. If the problem persists, it is recommended to contact *My Oracle Support (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, it is recommended to contact *My Oracle Support (MOS)* for assistance.

19832 - Communication Agent Reliable Transaction Failed

Event Type:	CAF
Description:	Failed transaction between servers result from normal maintenance actions, overload conditions, software failures, or equipment failures.

Severity: Info

Instance: <ServiceName>, <RemoteIP> | <null>

- If serviceID is InvalidServiceID, then <ServiceName> is "EventTransfer".
- If <ServiceName> is "EventTransfer", then include <RemoteIP>.
- If serviceID is unknown, then <ServiceName> is null.

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventComAgtTransFailedNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if the local server is unable to communicate with another server or if servers have become overloaded.
2. Check the server's KPIs and the **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to trouble-shoot the cause of server overload.
3. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **HA Status** that corresponds to the ServiceID in the event instance to trouble-shoot the operation of the service.
4. If the event cannot be explained by maintenance actions, it is recommended to contact *My Oracle Support (MOS)* for assistance.

19833 - Communication Agent Service Egress Message Discarded

Event Type: CAF

Description: Communication Agent Service Egress Message Discarded.

Severity: Info

Instance: <ServiceName>

- If serviceID is unknown, then <ServiceName> is null.

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventRoutingFailedNotify

Recovery:

1. View the Event AddlInfo column.

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

   If the condition is persistent with the status of one of the ComAgent Configuration Managed Objects there is an underlying issue with the Managed Object.
2. Use **Main Menu** > **Alarms & Events** and examine the alarm log for ComAgent Process problems.
3. It is recommended to contact *My Oracle Support (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. It is recommended to 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:	cAFEventSvcProvRegStateChangedNotify

Recovery:

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

19857 - Communication Agent Service Provider Operational State Changed

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

Recovery:

1. This event indicates that a ComAgent service provider changed operational state, and typically results from maintenance actions. A service can also change state due to overload.
2. If the state change is unexpected, it is recommended to contact *My Oracle Support (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, it is recommended to 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, it is recommended to contact *My Oracle Support (MOS)* for assistance.
4. If conditions permit, then initiate a failover of active NOAM.

   This causes the Communication Agent Configuration Daemon to exit on the originally-active NOAM and to start on the newly-active NOAM.

5. After NOAM failover completes, verify that the alarm has cleared.
6. If the alarm has not cleared, it is recommended to contact *My Oracle Support (MOS)* for assistance.

19861 - Communication Agent Configuration Daemon Script Failure

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, it is recommended to contact *My Oracle Support (MOS)* for assistance.
4. If conditions permit, then initiate a failover of active NOAM.

   This causes the Communication Agent Configuration Daemon to exit on the originally-active NOAM and to start on the newly-active NOAM.
5. After NOAM failover completes, verify that the alarm has cleared.
6. If the alarm has not cleared, it is recommended to contact *My Oracle Support (MOS)* for assistance.

19862 - Communication Agent Ingress Stack Event Rate

Alarm Group:	CAF
Description:	The Communication Agent Ingress Stack Event Rate is approaching its defined threshold capacity.
Severity:	• Minor - if exceeding 100K on Gen8/Gen9 hardware, 75k on other hardware • Major - if exceeding 110K on Gen8/Gen9 hardware, 80k on other hardware

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

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

Recovery:

1. This alarm indicates that a server is overrunning its defined processing capacity. If any of the defined threshold onset levels are exceeded, Communication Agent will discard comparatively low priority messages. Check the configuration, routing, and deployment mode capacity.
2. It is recommended to contact *My Oracle Support (MOS)* for further assistance.

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group:	CAF
Description:	The maximum number of connections per connection group limit has been reached.
Severity:	Info
Instance:	<Connection group name>
HA Score:	Normal
Throttle Seconds:	10
OID:	cAFComAgentMaxConnsInConnGrpNotify

Recovery:

1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.
2. It is recommended to contact *My Oracle Support (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, it is recommended to 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, it is recommended to 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:

- 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. It is recommended to 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.

19420 - BDFQFull

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

Severity	Minor
Instance	N/A
HA Score	Normal
Auto Clear Seconds	0 (zero)
OID	cAFBDFQFullNotify

Recovery:

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

19421 - BDFThrotl

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

Recovery:

It is recommended to contact *My Oracle Support (MOS)* for assistance if needed.

19422 - BDFInvalidPkt

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

Recovery:

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

19900 - DP Server CPU utilization

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

It is recommended to 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.

It is recommended to 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.

It is recommended to contact *My Oracle Support (MOS)* for assistance.

19904 - CFG-DB post-update Failure

Alarm Group: STK

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

Severity: Critical

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

Recovery:

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

It is recommended to contact *My Oracle Support (MOS)* for assistance.

19905 - Measurement Initialization Failure

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

Recovery:

Measurement subsystem initialization has failed for the specified measurement.

It is recommended to contact *My Oracle Support (MOS)* for assistance.

Platform (31000-32800)

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32800.

31000 - S/W fault

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

OID:	comcolSwFaultNotify

Recovery:

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

31001 - S/W status

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

Recovery:

No action required.

31002 - Process watchdog failure

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

Recovery:

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

31101 - Database replication to slave failure

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

Recovery:

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

31102 - Database replication from master failure

Alarm Group:	REPL

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

Recovery:

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

31103 - DB Replication update fault

Alarm Group:	REPL
Description:	Database replication process cannot apply update to DB.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepUpdateFaultNotify

Recovery:

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

31104 - DB Replication latency over threshold

Alarm Group:	REPL
Description:	Database replication latency has exceeded thresholds
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepLatencyNotify

Recovery:

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

31106 - Database merge to parent failure

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

Recovery:

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

31107 - Database merge from child failure

Alarm Group:	COLL
Description:	Database merging from a child Source Node has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMergeFromChildFailureNotify

Recovery:

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

31108 - Database merge latency over threshold

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

Recovery:

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

1. No action required.
2. It is recommended to 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:

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

31116 - Excessive shared memory

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

Recovery:

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

31117 - Low disk free

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

Recovery:

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

31118 - Database disk store fault

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

Recovery:

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

It is recommended to 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, it is recommended to 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. It is recommended to 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, it is recommended to 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. It is recommended to 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, it is recommended to 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, it is recommended to 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. It is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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. It is recommended to 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. It is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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. It is recommended to 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, it is recommended to 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:

1. This alarm indicates a system metric is configured incorrectly.
2. It is recommended to 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:

It is recommended to 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:

It is recommended to 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:

It is recommended to 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:

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

31224 - HA configuration error

Alarm Group:	HA
Description:	High availability configuration error
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

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

Recovery:

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

Recovery:

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

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, it is recommended to 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, it is recommended to 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, it is recommended to contact *My Oracle Support (MOS)*.

31283 - Lost Communication with server

Alarm Group:	HA
Description:	Highly available server failed to receive mate heartbeats

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

Recovery:

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

31284 - HA Remote Subscriber Heartbeat Warning

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

Recovery:

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

It is recommended to contact *My Oracle Support (MOS)* to request hardware replacement.

32101 - Breaker Panel Breaker Failure

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

Recovery

It is recommended to contact *My Oracle Support (MOS)* to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

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

Recovery

It is recommended to contact *My Oracle Support (MOS)* to request hardware replacement.

32103 - Power Feed Unavailable

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

Recovery

It is recommended to contact *My Oracle Support (MOS)* to request hardware replacement.

32104 - Power Supply 1 Failure

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

Recovery

It is recommended to contact *My Oracle Support (MOS)* to request hardware replacement.

32105 - Power Supply 2 Failure

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

Recovery

It is recommended to contact *My Oracle Support (MOS)* to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group:	PLAT
Description:	Power Supply 3 Failure
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply3Failure

Recovery

It is recommended to 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

It is recommended to 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

It is recommended to 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

It is recommended to 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

It is recommended to 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:

It is recommended to 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:

It is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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, it is recommended to 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:

```
cat /proc/mdstat
```

```
cat /etc/raidtab
```

3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output and collected data.

32302 - Server RAID disk error

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

Recovery

It is recommended to contact *My Oracle Support (MOS)*.

32303 - Server Platform error

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

Recovery:

1. Run syscheck in verbose mode.
2. Determine the raid state of the mirrored disks, collect data:

```
cat /proc/mdstat
```

```
cat /etc/raidtab
```

3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output and collected data.

32304 - Server file system error

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

Recovery:

1. Run syscheck in verbose mode.
2. Address full file systems identified in syscheck output, and run syscheck in verbose mode.
3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output.

32305 - Server Platform process error

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

Recovery:

1. Rerun syscheck in verbose mode.
2. If the alarm has been cleared then the problem is solved..
3. If the alarm has not been cleared then determine the run level of the system.
4. If system run level is not 4 then determine why the system is operating at that run level.
5. If system run level is 4, determine why the required number of instances process(es) are not running.
6. If the alarm persists, it is recommended to contact *My Oracle Support (MOS)* and provide the system health check output.

32306 - Server RAM shortage error

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

Recovery

It is recommended to contact *My Oracle Support (MOS)*.

32307 - Server swap space shortage failure

Alarm Group:	PLAT

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

Recovery:

1. Run syscheck in verbose mode.
2. Determine processes using swap.

   Note: One method to determine the amount of swap being used by process is:

```
grep VmSwap /proc/<process id>/status
```

3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output and process swap usage.

32308 - Server provisioning network error

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

Recovery:

1. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.
2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.

4. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, it is recommended to contact *My Oracle Support (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

It is recommended to 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

It is recommended to 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

It is recommended to 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: • A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system. • More than 90% of the total number of available files have been allocated on the file system. • A file system has a different number of blocks than it had when installed.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskSpaceShortageError
Alarm ID:	TKSPLATMA13

Recovery:

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

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDefaultRouteNetworkError

Recovery:

1. Run syscheck in verbose mode.
2. If the syscheck output is: `The default router at <IP_address> cannot be pinged`, the router may be down or unreachable. Do the following:
   a) Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
   b) Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
   c) Check with the router administrator to verify that the router is configured to reply to pings on that interface.
   d) Rerun syscheck.
   e) If the alarm has not been cleared, it is recommended to collect the syscheck output and contact *My Oracle Support (MOS)*.
3. If the syscheck output is: `The default route is not on the provisioning network`, it is recommended to collect the syscheck output and contact *My Oracle Support (MOS)*.
4. If the syscheck output is: `An active route cannot be found for a configured default route`, it is recommended to collect the syscheck output and contact *My Oracle Support (MOS)*.

32314 - Server temperature error

Alarm Group: PLAT

Description: The internal temperature within the server is unacceptably high.

Severity: Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerTemperatureError
Alarm ID:	TKSPLATMA15

Recovery:

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

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

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

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

5. Re-run syscheck.
   a) If the alarm has been cleared, the problem is resolved.
   b) If the alarm has not been cleared, continue troubleshooting.
6. If the problem has not been resolved, it is recommended to contact *My Oracle Support (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 the alarm persists, it is recommended to 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, it is recommended to 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, it is recommended to 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. It is recommended to 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

It is recommended to 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, it is recommended to contact *My Oracle Support (MOS)* and provide the system health check output and the output of the above investigation.

32321 - Correctable ECC memory error

Alarm Group:	PLAT
Description:	This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdEccCorrectableError
Alarm ID:	TKSPLATMA22

Recovery:

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

32322 - Power Supply A error

Alarm Group:	PLAT
Description:	This alarm indicates that power supply 1 (feed A) has failed.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply1Error
Alarm ID:	TKSPLATMA23

Recovery:

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

32323 - Power Supply B error

Alarm Group:	PLAT
Description:	This alarm indicates that power supply 2 (feed B) has failed.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply2Error
Alarm ID:	TKSPLATMA24

Recovery:

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

32324 - Breaker panel feed error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not receiving information from the breaker panel relays.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdBrkPnlFeedError
Alarm ID:	TKSPLATMA25

Recovery:

1. Verify that the same alarm is displayed by multiple servers:
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.
3. If the problem has not been resolved, it is recommended to contact *My Oracle Support (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 15: 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.

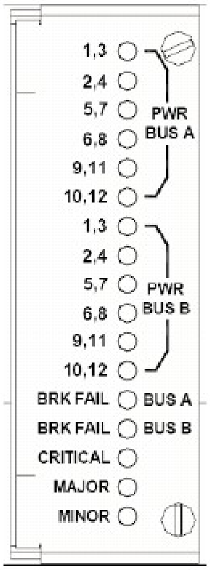


Figure 15: Breaker Panel LEDs

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.

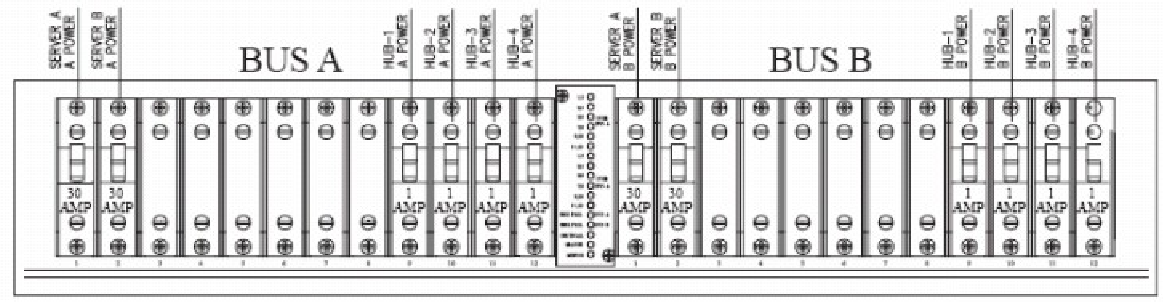


Figure 16: Breaker Panel Setting

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 it is recommended to run syscheck and contact *My Oracle Support (MOS)*
5. Run syscheck.
   - If the alarm has been cleared, the problem is resolved.
   - If the problem has not been resolved, it is recommended to contact *My Oracle Support (MOS)*

32326 - Breaker panel monitoring error

Alarm Group: PLAT

Description: This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself.

Note: When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm:

- 32324 – Breaker panel feed error
- 32325 – Breaker panel breaker error

until the Breaker Panel Monitoring Error has been corrected.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlMntError

Alarm ID: TKSPLATMA27

Recovery:

1. Verify that the same alarm is displayed by both servers (the single breaker panel normally sends alarm information to both servers):

- If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
- If this alarm is displayed by both servers, go to the next step.

2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).
3. Run syscheck..
    - If the alarm has been cleared, the problem is resolved.
    - If the alarm has not been cleared, it is recommended to contact *My Oracle Support (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 heartbeart is running (service TKLCha status).

    Note: This step may require command line ability.

4. It is recommended to contact *My Oracle Support (MOS)*.

32328 - DRBD is unavailable

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

It is recommended to 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

It is recommended to 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

It is recommended to 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 the condition persists, it is recommended to contact *My Oracle Support (MOS)* and provide the system health check output. The disk may need to be replaced.

32332 - HP Smart Array controller problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskCtrlrProblem
Alarm ID:	TKSPLATMA33

Recovery:

1. Run syscheck in verbose mode.
2. If condition persists, it is recommended to contact *My Oracle Support (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. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output, and savelogs_plat output.

32334 - Multipath device access link problem

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:

It is recommended to 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, it is recommended to contact *My Oracle Support (MOS)* to determine who should verify port settings on both the server and the switch.

32336 - Half Open Socket Limit

Alarm Group:	PLAT
Description:	This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHalfOpenSockLimit

Alarm ID:	TKSPLATMA37

Recovery:

1. Run syscheck in verbose mode.
2. Determine what process and address reports a state of SYN_RECV and collect data:
   - netstat -nap.
3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output and collected data.

32337 - Flash Program Failure

Alarm Group:	PLAT
Description:	This alarm indicates that there was an error while trying to update the firmware flash on the E5-APP-B cards.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdFlashProgramFailure
Alarm ID:	TKSPLATMA38

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32338 - Serial Mezzanine Unseated

Alarm Group:	PLAT
Description:	This alarm indicates that a connection to the serial mezzanine board may not be properly seated.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSerialMezzUnseated
Alarm ID:	TKSPLATMA39

Recovery:

1. Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.

2. It is recommended to contact *My Oracle Support (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. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output, and pid output.

32340 - TPD NTP Daemon Not Synchronized Error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedError
Alarm ID:	TKSPLATMA41

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a) Ensure ntpd service is running.
   b) Verify the content of the /etc/ntp.conf file is correct for the server.

c) Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.

d) Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.

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

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

   a) To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

4. If the problem persists, it is recommended to contact *My Oracle Support (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 the ntp peer is reachable, restart the ntpd service.
3. If the problem persists then a reset the NTP date may resolve the issue.

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

a) To reset date:

- sudo service ntpd stop
- sudo ntpdate <ntp server ip>
- sudo service ntpd start

4. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

32342 - NTP Offset Check Error

Alarm Group:	PLAT
Description:	This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpOffsetCheckError
Alarm ID:	TKSPLATMA43

Recovery:

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

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

   a) To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

4. If the problem persists, it is recommended to contact *My Oracle Support (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. It is recommended to 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. It is recommended to 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 the alarm persists, it is recommended to 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. It is recommended to 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:	tpdHWMGMTCLIProblem
Alarm ID:	TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the hwmgmtd process is running. If not running verify that it was not administratively stopped.
   - Executing "service hwmgmtd status" should produce output indicating that the process is running.
   - If not running attempt to start process "service hwmgmtd status".
4. Determine if the TKLChwmgmtcli process is running. If not running verify that it was not administratively stopped.
   - Executing "status TKLChwmgmtcli" should produce output indicating that the process is running.
   - If not running attempt to start process "start TKLChwmgmtcli".
5. Verify that there are no hwmgmt error messages in /var/log/messages. If there are this could indicate that the Oracle utility is hung. If hwmgmtd process is hung, proceed with next step.
6. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output.

32348 - FIPS Subsystem Problem

Alarm Type: PLAT

Description: This alarm indicates that the FIPS subsystem is not running or has encountered errors.

Default Severity: Major

OID: tpdFipsSubsystemProblem

Recovery

1. Run syscheck in verbose mode.
2. Contact *My Oracle Support (MOS)*.

32349 - File Tampering

Alarm Group:	PLAT
Description:	This alarm indicates HIDS has detected file tampering.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHidsFileTampering

Recovery:

It is recommended to 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:

- A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system.
- More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskSpaceShortageWarning

Alarm ID: TKSPLATMI1

Recovery:

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

It is recommended to 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. It is recommended to contact *My Oracle Support (MOS)*, provide the system health check output, and process swap usage.

32506 - Server default router not defined

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

Caution: When changing the server's network routing configuration it is important to verify that the modifications will not impact the method of connectivity for the current login session. It is also crucial that this information not be entered incorrectly or set to improper values. Incorrectly modifying the server's routing configuration may result in total loss of remote network access.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDefaultRouteNotDefined

Alarm ID: TKSPLATMI7

Recovery:

1. Run syscheck in verbose mode.
2. If the syscheck output is: `The default router at <IP_address> cannot be pinged`, the router may be down or unreachable. Do the following:
   a) Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
   b) Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
   c) Check with the router administrator to verify that the router is configured to reply to pings on that interface.
   d) Rerun syscheck.
3. If the alarm has not cleared, it is recommended to collect the syscheck output and contact *My Oracle Support (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, it is recommended to 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. It is recommended to contact *My Oracle Support (MOS)* to create a service request.
2. On the affected server, execute this command:

   ```
   ll /var/TKLC/core
   ```

   Add the command output to the service request. Include the date of creation found in the command output.
3. Attach core files to the *My Oracle Support (MOS)* service request.
4. The user can remove the files to clear the alarm with this command:

   ```
   rm -f /var/TKLC/core/<coreFileName>
   ```

32509 - Server NTP Daemon not synchronized

Alarm Group:	PLAT
Description:	This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDeamonNotSynchronizedWarning
Alarm ID:	TKSPLATMI10

Recovery:

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

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

   a) To reset date:

- sudo service ntpd stop
- sudo ntpdate <ntp server ip>
- sudo service ntpd start

4. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

32510 - CMOS battery voltage low

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:

It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to contact *My Oracle Support (MOS)*.

32514 - Server reboot watchdog initiated

Alarm Group:	PLAT
Description:	This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies

	to only the last reboot and is only supported on a T1100 application server.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdWatchdogReboot
Alarm ID:	TKSPLATMI15

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32515 - Server HA failover inhibited

Alarm Group:	PLAT
Description:	This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaInhibited
Alarm ID:	TKSPLATMI16

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32516 - Server HA Active to Standby transition

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:

It is recommended to 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:

It is recommended to 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:

It is recommended to contact *My Oracle Support (MOS)*.

32519 - NTP Offset Check failure

Alarm Group:	PLAT
Description:	This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message

	will provide the offset value of the server from the NTP server and the offset limit that the application has set for the system.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpOffsetCheckWarning
Alarm ID:	TKSPLATMI20

Recovery:

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

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

   a) To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start
4. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

32520 - NTP Stratum Check failure

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, it is recommended to 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:

It is recommended to contact *My Oracle Support (MOS)* to get a replacement sensor.

32522 - SAS Drive Missing

Alarm Group:	PLAT

Description: This alarm indicates that the number of drives configured for this server is not being detected.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: sasDriveMissing

Alarm ID: TKSPLATMI23

It is recommended to 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, it is recommended to contact *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:

1. Run syscheck in verbose mode.
2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck.
3. If the alarm persists, it is recommended to contact *My Oracle Support (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:

Contact the vendor to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.

Note: *My Oracle Support (MOS)* personnel can perform an `snmpget` command or log into the switch to get detailed fan status information.

32526 - Telco Temperature Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoTemperatureWarning
Alarm ID:	TKSPLATMI27

Recovery:

1. Lower the ambient air temperature around the switch as low as possible.
2. If the problem persists, it is recommended to contact *My Oracle Support (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 the breaker is still good and problem persists, it is recommended to contact *My Oracle Support (MOS)* who can perform a `snmpget` command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 - Invalid BIOS value

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. It is recommended to 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:

1. Run syscheck in verbose mode.
2. It is recommended to 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:	TpdServerUpgradeFailed
Alarm ID:	TKSPLATMI31

Recovery:

It is recommended to 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. It is recommended to 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. It is recommended to 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, it is recommended to 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:

1. Run syscheck in verbose mode.
2. If this alarm persists for several hours (depending on a load of a server, rebuilding an array can take multiple hours to finish), it is recommended to contact *My Oracle Support (MOS)*.

32536 - TPD Server Upgrade snapshot(s) warning

Alarm Group: PLAT

Description: This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdUpgradeSnapshotWarning

Alarm ID: TKSPLATMI37

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. It is recommended to contact *My Oracle Support (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, it is recommended to contact *My Oracle Support (MOS)*.

32540 - CPU Power limit mismatch

Alarm Group:	PLAT
Description:	The BIOS setting for CPU Power Limit is different than expected.
Severity:	Minor
Instance:	N/A
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdCpuPowerLimitMismatch
Alarm ID:	TKSPLATMI41

Recovery:

It is recommended to 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
Auto Clear Seconds	86400

OID	tpdTelcoSwitchNotification

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32701 - HIDS Initialized

Alarm Group:	PLAT
Description:	This alarm indicates HIDS was initialized.
Default Severity:	Info
OID:	tpdHidsBaselineCreated

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32702 - HIDS Baseline Deleted

Alarm Group:	PLAT
Description:	HIDS baseline was deleted.
Default Severity:	Info
OID:	tpdHidsBaselineDeleted

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32703 - HIDS Enabled

Alarm Group:	PLAT
Description:	HIDS was enabled.
Default Severity:	Info
OID:	tpdHidsEnabled

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32704 - HIDS Disabled

Alarm Group:	PLAT
Description:	HIDS was disabled.
Default Severity:	Info
OID:	tpdHidsDisabled

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32705 - HIDS Monitoring Suspended

Alarm Group:	PLAT
Description:	HIDS monitoring suspended.
Default Severity:	Info
OID:	tpdHidsSuspended

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32706 - HIDS Monitoring Resumed

Alarm Group:	PLAT
Description:	HIDS monitoring resumed.
Default Severity:	Info
OID:	tpdHidsResumed

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

32707 - HIDS Baseline Updated

Alarm Group:	PLAT
Description:	HIDS baseline updated.
Default Severity:	Info
OID:	tpdHidsBaselineUpdated

Recovery:

It is recommended to contact *My Oracle Support (MOS)*.

Chapter

5

Key Performance Indicators (KPIs)

Topics:

- *General KPIs information.....219*
- *KPIs server elements 221*
- *Provisioning KPIs.....222*
- *Process-based KPIs.....223*
- *DP KPIs.....224*
- *Communication Agent (ComAgent) KPIs.....225*

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 the **KPI Filter** button and specify filter options using the drop-down menus to see KPI data relevant to an application.
3. Click to select an application tab to see KPI data relevant to the application.**Go** to filter on the selection.

   Note: The application KPIs displayed may vary according to whether you are logged in to an NOAM server or an SOAM server. Collection of KPI data is handled solely by NOAM servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the **KPIs > Export** page.

Table 16: 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 transfered 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 *Viewing the file list*.

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

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

KPIs server elements

This table describes KPIs that appear regardless of server role.

Table 17: KPIs Server Elements

KPIs Status Element	Description
Network Element	The network element name (set up on the **Configuration** > **Network Elements** page) associated with each Server Hostname.
Server Hostname	The server hostname set up on the **Configuration** > **Servers** page. All servers in the system are listed here.
Server Indicators:	
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system.

KPIs Status Element	Description
RAM	Percentage utilization of physical memory on the server by all software as measured by TPD.
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.
Uptime	The total amount of time the server has been running.

Provisioning KPIs

Table 18: Provisioning KPIs

Variable	Description
ProvConnections	The number of provisioning client connections currently established. A single connection includes a client having successfully established a TCP/IP connection, sent a provisioning connect message, and having received a successful response.
ProvMsgsReceived	The number of provisioning messages per second that have been received from all sources except import files.
ProvMsgsImported	The number of provisioning messages per second imported from files.
ProvMsgsSuccessful	The number of provisioning messages per second that have been successfully processed and a success response sent to the requestor.
ProvMsgsFailed	The number of provisioning messages per second that have failed to be processed due to errors and a failure response sent to the requestor.
ProvMsgsSent	The number of provisioning message responses sent per second to the requestor.
ProvMsgsDiscarded	The number of provisioning messages discarded per second. provisioning messages are discarded due to connection shutdown, server shutdown, server‘s role switching from active to standby, or transaction not becoming durable within the allowed amount of time.
ProvTxnCommitted	The number of provisioning transactions per second that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS cluster.
ProvTxnFailed	The number of provisioning transactions per second that have failed to be started, committed, or aborted due to errors.
ProvTxnAborted	The number of provisioning transactions aborted per second.

Variable	Description
ProvTxnActive	The number of provisioning transactions that are currently active (normal transaction mode only).
ProvTxnNonDurable	The number of transactions that have been committed, but are not yet durable. Responses for the associated requests are not sent until the transaction has become durable.
ProvRelayMsgsSent	The number of relayed provisioning messages sent per second.
ProvRelayMsgsSuccessful	The number of relayed provisioning messages per second that were successful at the HLRR.
ProvRelayMsgsFailed	The number of relayed provisioning messages per second that failed at the HLRR.
ProvRemoteAuditMsgsSent	The number of IMSI and MSISDN records audited per second.
ProvRelayTimeLag	Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.
ProvDbException	The number of DB Exception errors per second.

Process-based KPIs

Table 19: Process-based KPIs

Variable	Description
provimport.Cpu	CPU usage of provimport process
provimport.MemHeap	Heap memory usage of provimport process
provimport.MemBasTotal	Memory usage of provimport process
provimport.MemPerTotal	Percent memory usage of provimport process
provexport.Cpu	CPU usage of provexport process
provexport.MemHeap	Heap memory usage of provexport process
provexport.MemBasTotal	Memory usage of provexport process
provexport.MemPerTotal	Percent memory usage of provexport process
pdbrelay.Cpu	CPU usage of pdbrelay process
pdbrelay.MemHeap	Heap memory usage of pdbrelay process
pdbrelay.MemBasTotal	Memory usage of the pdbrelay process
pdbrelay.MemPerTotal	Percent memory usage of pdbrelay process
pdbaudit.Cpu	CPU usage of pdbaudit process

Variable	Description
pdbaudit.MemHeap	Heap memory usage of pdbaudit process
pdbaudit.MemBasTotal	Memory usage of the pdbaudit process
pdbaudit.MemPerTotal	Percent memory usage of pdbaudit process
pdba.Cpu	CPU usage of pdba process
pdba.MemHeap	Heap memory usage of pdba process
pdba.MemBasTotal	Memory usage of pdba process
pdba.MemPerTotal	Percent memory usage of pdba process
xds.Cpu	CPU usage of xds process
xds.MemHeap	Heap memory usage of xds process
xds.MemBasTotal	Memory usage of xds process
xds.MemPerTotal	Percent memory usage of xds process
dpserver.Cpu	CPU usage of dpserver process on DP
dpserver.MemHeap	Heap memory usage of dpserver process on DP
dpserver.MemBaseTotal	Memory usage of the dpserver process on DP
dpserver.MemPerTotal	Percent memory usage of dpserver on DP
era.Cpu	CPU usage of era process
era.MemHeap	Heap memory usage of era process
era.MemBasTotal	Memory usage of era process
era.MemPerTotal	Percent memory usage of era process

DP KPIs

Table 20: DP KPIs

Variable	Description
DpsQueryRate	Total number of queries received per second
DpsMsisdnQueryRate	Total number of MSISDN queries received per second
DpsImsiQueryRate	Total number of IMSI queries received per second
DpsNaiQueryRate	Total number of NAI queries received per second
DpsFailedQueryRate	Total number of queries failed per second

Variable	Description
DpsNotFoundQueryRate	Total number of queries with Not Found responses per second
DpsMsisdnNotFoundQueryRate	Total number of MSISDN queries with Not Found responses per second
DpsImsiNotFoundQueryRate	Total number of IMSI queries with Not Found responses per second
DpsNaiNotFoundQueryRate	Total number of NAI queries with Not Found responses per second
DpsResponseSent	Total number of responses sent per second
DpsIngressQueue	DP Ingress Queue percentage full
DpsMsisdnBlacklistedRate	Total number of MSISDN Queries with Blacklisted Responses per second
DpsImsiBlacklistedRate	Total number of IMSI Queries with Blacklisted Responses per second

Communication Agent (ComAgent) KPIs

The KPI values associated with ComAgent are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 21: Communication Agent KPIs

Variable	Description
User Data Ingress message rate	The number of User Data Stack Events received by ComAgent.
Broadcast Data Rate	The overall data broadcast rate on the server.

Chapter 6

Measurements

Topics:

- *General measurements information.....227*
- *Provisioning interface measurements.....231*
- *DP Measurements.....244*
- *Communication Agent (ComAgent) Performance measurements.....256*
- *Communication Agent (ComAgent) Exception measurements.....274*
- *OAM.ALARM measurements.....304*
- *OAM.SYSTEM measurements.....305*

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 22: 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: • 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**.

   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 23: 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 *Viewing the file list*.

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

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

Provisioning interface measurements

The provisioning interface measurement group is a set of measurements associated with the usage of provisioning Rules. These measurements will allow the user to determine which provisioning Rules are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed.

Table 24: Application Routing Rule Measurements

Measurement Tag	Description	Collection Interval
ProvConnectsAttempted	The total number of client initiated connect attempts to establish a connection with the server.	5 min
ProvConnectsAccepted	The total number of client initiated connect attempts that have been accepted.	5 min
ProvConnectsDenied	The 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 provisioning interface is disabled.	5 min
ProvConnectsFailed	The total number of client initiated connect attempts that failed due to errors during initialization.	5 min
ProvConnectionIdleTimeouts	The total number of connections that have timed out and terminated due to idleness.	5 min
ProvMsgsReceived	The total number of provisioning messages that have been received from all sources (except import files).	5 min
ProvMsgsSuccessful	The total number of provisioning messages that have been successfully processed and a success response sent to the requestor.	5 min

Measurement Tag	Description	Collection Interval
ProvMsgsFailed	The total number of provisioning messages that have failed to be processed due to errors and a failure response sent to the requestor.	5 min
ProvMsgsSent	The total number of provisioning messages for which a response has been sent to the requestor.	5 min
ProvMsgsDiscarded	The total number of provisioning messages that have been discarded (instead of sending a reply to the requestor) 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
ProvMsgsImported	The total number of provisioning messages that have been received from a file import operation.	5 min
ProvTxnCommitted	The total number of transactions that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS site.	5 min
ProvTxnWriteMutexTimeouts	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
ProvTxnFailed	The total number of transactions that have failed to be started, committed, or aborted due to errors.	5 min
ProvTxnAborted	The total number of transactions that have been successfully aborted.	5 min
ProvTxnTotal	The total number of transactions that have been attempted. It is the sum of ProvTxnCommitted, ProvTxnTimeouts, ProvTxnAborted, and ProvTxnFailed counters.	5 min
ProvTxnDurabilityTimeouts	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
ProvRelayMsgsSent	The total number of relayed provisioning messages sent to the remote system.	5 min
ProvRelayMsgsSuccessful	The total number of relayed provisioning messages that have been successfully processed on the remote system.	5 min
ProvRelayMsgsFailed	The total number of relayed provisioning messages that have failed to be processed due to errors on the remote system.	5 min
ProvImportsSuccessful	The number of files imported successfully.	5 min

Measurement Tag	Description	Collection Interval
ProvImportsFailed	The number of files that failed to be imported due to errors.	5 min
ProvExportsSuccessful	The number of successful file export requests.	5 min
ProvExportsFailed	The number of file export requests that failed due to errors.	5 min
ProvDnSplitCreated	Number of MSISDN records successfully created by a Split Activation starting its PDP.	5 min
ProvDnSplitRemoved	Number of MSISDN records successfully removed by a Split Completing its PDP.	5 min
ProvNpaSplitStarted	Number of NPA split records successfully starting a PDP.	5 min
ProvNpaSplitCompleted	Number of NPA split records successfully completing a PDP.	5 min
ProvRemoteAuditMsgsSent	Number of IMSI and MSISDN records audited.	5 min
ProvRelayTimeLag	Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.	5 min
ProvDbException	Number of DB Exception errors.	5 min
RemoteAuditStarted	Number of started remote audit requests.	5 min
RemoteAuditCompleted	Number of successfully completed remote audit requests.	5 min

ProvConnectsAttempted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of client initiated connect attempts to establish a connection with the server.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvConnectsAccepted

Measurement Group	Provisioning Rules

Measurement Type	Simple
Description	The total number of client initiated connect attempts that have been accepted.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvConnectsDenied

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The 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 provisioning interface is disabled.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvConnectsFailed

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of client initiated connect attempts that failed due to errors during initialization.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvConnectionIdleTimeouts

Measurement Group	Provisioning Rules

Measurement Type	Simple
Description	Total number of connections that have timed out and terminated due to idleness.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvMsgsReceived

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of PROVISIONING messages that have been received from all sources (except import files).
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvMsgsSuccessful

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of PROVISIONING messages that have been successfully processed and a success response sent to the requestor.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvMsgsFailed

Measurement Group	Provisioning Rules

Measurement Type	Simple
Description	The total number of PROVISIONING messages that have failed to process due to errors and a failure response sent to the requestor.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvMsgsSent

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of PROVISIONING messages that have been sent and a response sent to the requestor.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvMsgsDiscarded

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of PROVISIONING messages that have been discarded (instead of sending a reply to the requestor) 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.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvMsgsImported

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of PROVISIONING messages that have been received from a file import operation.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvTxnCommitted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of transactions that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS site.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvTxnWriteMutexTimeouts

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvTxnFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of transactions that have failed to be started, committed, or aborted due to errors.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnAborted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of transactions that have been successfully aborted.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvTxnTotal

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of transactions that have been attempted. It is the sum of ProvTxnCommitted, ProvTxnTimeouts, ProvTxnAborted, and ProvTxnFailed counters.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvTxnDurabilityTimeouts

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of committed, non-durable transaction that have failed to become durable within the amount of time specified by Transaction Durability Timeout.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvRelayMsgsSent

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of relayed PROVISIONING messages sent to the remote system.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvRelayMsgsSuccessful

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of relayed PROVISIONING messages that have been successfully processed on the remote system.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvRelayMsgsFailed

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The total number of relayed PROVISIONING messages that have failed to be processed due to errors on the remote system.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvImportsSuccessful

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The number of files imported successfully.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvImportsFailed

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The number of files that failed to be imported due to errors.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvExportsSuccessful

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The number of successful CSV/XML file export requests.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvExportsFailed

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	The number of CSV/XML file export requests that failed due to errors.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvDnSplitCreated

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of DN records successfully created by an Active Split.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvDnSplitRemoved

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of DN records successfully removed by a Split Completing its PDP.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvNpaSplitStarted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of NPA split records successfully starting a PDP.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvNpaSplitCompleted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of NPA split records successfully completing a PDP.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvRemoteAuditMsgsSent

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of IMSI and MSISDN records audited.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvRelayTimeLag

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

ProvDbException

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of DB Exception errors.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

RemoteAuditCompleted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of successfully completed remote audit requests.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

RemoteAuditStarted

Measurement Group	Provisioning Rules
Measurement Type	Simple
Description	Number of started remote audit requests.
Collection Interval	5 min
Peg Condition	
Measurement Scope	PROV Group

Recovery

No action required.

DP Measurements

Table 25: DP Measurements

Measurement Tag	Description	Collection Interval
DpsQueriesReceived	Number of Queries received	5 minutes
DpsMsisdnQueriesReceived	Number of MSISDN Queries received	5 minutes
DpsImsiQueriesReceived	Number of IMSI Queries received	5 minutes
DpsNaiQueriesReceived	Number of NAI Queries received	5 minutes
DpsQueriesFailed	Number of Queries failed	5 minutes
DpsMsisdnQueriesFailed	Number of MSISDN Queries with Fail response	5 minutes

Measurement Tag	Description	Collection Interval
DpsImsiQueriesFailed	Number of IMSI Queries with Fail response	5 minutes
DpsNaiQueriesFailed	Number of NAI Queries with Fail response	5 minutes
DpsSuccessResponses	Number of Queries with Success response	5 minutes
DpsMsisdnSuccessResponses	Number of MSISDN Queries with Success response	5 minutes
DpsImsiSuccessResponses	Number of IMSI Queries with Success response	5 minutes
DpsNaiSuccessResponses	Number of NAI Queries with Success response	5 minutes
DpsNotFoundReponses	Number of Queries with Not Found response	5 minutes
DpsMsisdnNotFoundResponses	Number of MSISDN Queries with Not Found response	5 minutes
DpsImsiNotFoundResponses	Number of IMSI Queries with Not Found response	5 minutes
DpsNaiNotFoundResponses	Number of NAI Queries with Not Found response	5 minutes
DpsRespSent	Total number of responses sent	5 minutes
DpsIngressQueuePeak	Peak DPS Ingress Queue utilization during collection period	5 minutes
DpsIngressQueueAvg	Average DPS Ingress Queue utilization during the collection period	5 minutes
DpsIngressQueueFull	Number of DPS Ingress Queue StackTask messages discarded during the collection period because the number of message queued exceeded the maximum capacity	5 minutes
DpsQueryRatePeak	Peak Ingress Message Rate in messages per second during the collection period	5 minutes
DpsQueryRateAvg	Average Ingress Message Rate in messages per second during the collection period	5 minutes
DpsQueryProcessingTime	Distribution of times (in microseconds) taken by dpserver to process each query and send its reply.	5 minutes
DpsQueryProcessingTimeAvg	The average query processing time (in microseconds) taken by dpserver to process each query and sent its reply.	5 minutes
DpsMsisdnBlacklistedResponses	Number of MSISDN Queries with Blacklisted response	5 minutes

Measurement Tag	Description	Collection Interval
DpsImsiBlacklistedResponses	Number of IMSI Queries with Blacklisted response	5 minutes
DpsMsisdnPrefixFound	Number of MSISDN Queries that were found by matching a prefix	5 minutes
DpsImsiPrefixFound	Number of IMSI Queries that were found by matching a prefix	5 minutes
DpsMsisdnBlacklistLookups	Number of MSISDN Blacklist Lookups performed	5 minutes
DpsImsiBlacklistLookups	Number of IMSI Blacklist Lookups performed	5 minutes
DpsMsisdnPrefixLookups	Number of MSISDN Prefix Lookups performed	5 minutes
DpsImsiPrefixLookups	Number of IMSI Prefix Lookups performed	5 minutes

DpsQueriesReceived

Measurement Group	DP
Measurement Type	Simple
Description	Number of Queries received
Collection Interval	5 min
Peg Condition	
Measurement Scope	DP Group

Recovery

No action required.

DpsMsisdnQueriesReceived

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Queries received
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiQueriesReceived

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Queries received
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsNaiQueriesReceived

Measurement Group	DP
Measurement Type	Simple
Description	Number of NAI Queries received
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsQueriesFailed

Measurement Group	DP
Measurement Type	Simple
Description	Number of Queries failed
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnQueriesFailed

Measurement Group	DP
Measurement Type	Simple

Description	Number of MSISDN Queries with Fail response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiQueriesFailed

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Queries with Fail response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsNaiQueriesFailed

Measurement Group	DP
Measurement Type	Simple
Description	Number of NAI Queries with Fail response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsSuccessResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of Queries with Success response
Collection Interval	5 min
Peg Condition	

Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnSuccessResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Queries with Success response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiSuccessResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Queries with Success response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsNaiSuccessResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of NAI Queries with Success response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsNotFoundResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of Queries with Not Found response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnNotFoundResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Queries with Not Found response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiNotFoundResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Queries with Not Found response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsNaiNotFoundResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of NAI Queries with Not Found response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsRespSent

Measurement Group	DP
Measurement Type	Simple
Description	Total number of responses sent
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsIngressQueuePeak

Measurement Group	DP
Measurement Type	Simple
Description	Peak DPS Ingress Queue utilization during collection period
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsIngressQueueAvg

Measurement Group	DP
Measurement Type	Simple
Description	Average DPS Ingress Queue utilization during collection period
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsIngressQueueFull

Measurement Group	DP
Measurement Type	Simple
Description	Number of DPS Ingress Queue Stack Task messages discarded during the collection period because the number of messages queued exceeded the maximum capacity
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsQueryRatePeak

Measurement Group	DP
Measurement Type	Simple
Description	Peak Ingress Message Rate in messages per second during the collection period
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsQueryRateAvg

Measurement Group	DP
Measurement Type	Simple
Description	Average Ingress Message Rate in messages per second during the collection period
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsQueryProcessingTime

Measurement Group	DP
Measurement Type	Simple
Description	Distribution of times (in microseconds) taken by dpserver to process each query and send its reply
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsQueryProcessingTimeAvg

Measurement Group	DP
Measurement Type	Simple
Description	The average query processing time (in microseconds) taken by dpserver to process each query and send its reply
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnBlacklistedResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Queries with Blacklisted response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiBlacklistedResponses

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Queries with Blacklisted response
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnPrefixFound

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Queries that were found by matching a prefix
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiPrefixFound

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Queries that were found by matching a prefix
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnBlacklistLookups

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Blacklist Lookups performed
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiBlacklistLookups

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Blacklist Lookups performed
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsMsisdnPrefixLookups

Measurement Group	DP
Measurement Type	Simple
Description	Number of MSISDN Prefix Lookups performed
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

DpsImsiPrefixLookups

Measurement Group	DP
Measurement Type	Simple
Description	Number of IMSI Prefix Lookups performed
Collection Interval	5 min
Peg Condition	
Measurement Scope	Data Processor

Recovery

No action required.

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 26: 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

Measurement Tag	Description	Collection Interval
CAAvgRsrcPoolUtil	Average percentage of internal resource pool utilization	30 min
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
CAPeakDataFIF0QueueUtil	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

Measurement Tag	Description	Collection Interval
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
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. It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to 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

CARxSuccess

Measurement Group	ComAgent Performance

Measurement Type	Simple
Measurement Dimension	Single
Description	Number of User Data ingress events successfully routed to local layers.
Collection Interval	30 min
Peg Condition	For each User Data StackEvent received from a peer server and successfully transmitted to the local stack.
Measurement Scope	NE, Server

Recovery

No action required.

This value provides a measure of how many User Data ingress messages are received by Communication Agent and are successfully transmitted to local hosting stack.

CATransEndAbnorm

Measurement Group	ComAgent Exception, ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (by Service ID)
Description	Number of reliable transactions that terminated abnormally.
Collection Interval	30 min
Peg Condition	• Transaction times-out waiting for a response, and the maximum number of transmits has been reached. • Transaction time-to-live limit is exceeded. • Transaction terminated due to lack of resources. **Note:** This measurement is NOT pegged for these conditions: • Transaction involves an unknown service. • Transaction involves an unregistered Routed Service.
Measurement Scope	Server

Recovery

1. Check the ComAgent Exception report to further diagnose the reasons why transactions are failing.
2. It is recommended to contact *My Oracle Support (MOS)* for assistance.

CATransEndAbnormRateAvg

Measurement Group	ComAgent Performance, ComAgent Exception
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 a sliding-metric 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 troubleshooting when compared to other measurements.
Measurement Scope	Server

Recovery

No action necessary.

CATransEndAbnormRateMax

Measurement Group	ComAgent Performance, ComAgent Exception
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 a sliding-metric 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 troubleshooting 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 a sliding-metric 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 troubleshooting 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 a sliding-metric 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 troubleshooting 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.

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.

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 27: Communication Agent Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
CADataFIFOQueueFul	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
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
CAMxFIFOQueueFul	StackEvents discarded due to ComAgent MxFIFO 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

Measurement Tag	Description	Collection Interval
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
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

Measurement Tag	Description	Collection Interval
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
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

Measurement Tag	Description	Collection Interval
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
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

CADataFIFOQueueFul

Measurement Group ComAgent Exception

Measurement Type Simple

Measurement Dimension Single

Description StackEvents discarded due to ComAgent DataFIFO queue full condition. This value provides a measure of how many messages

	are discarded by ComAgent due to ComAgent User Data FIFO Queue full condition.
Collection Interval	30 min
Peg Condition	For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent User Data FIFO queue.
Measurement Scope	NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to 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. It is recommended to 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. It is recommended to 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, it is recommended to contact *My Oracle Support (MOS)*.

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 pproduct'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. It is recommended to 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, it is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to 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

1. 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.
2. It is recommended to 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

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. It is recommended to contact *My Oracle Support (MOS)* for assistance.

CARsrcPoolFul

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Single
Description	ComAgent internal resource pool exhaustion condition.
Collection Interval	30 min
Peg Condition	This is to track the measure of the internal resource (Ex: CommMessage Resource pool) exhaustion condition for a given interval. For each resource allocation/access attempt that result in resource pool manager returning an indication that the maximum resources reserved are allocated and are in-use. When this condition occurs ComAgent tries to allocate a new resource from heap and relists it after its life cycle (Ex: CommMessage objects required for user data traffic for MxEndpoint interface).
Measurement Scope	NE, Server

Recovery

This value provides a measure of how many times pre-allocated resources are exhausted in ComAgent interfaces.

This measurement is primarily intended for performance analysis and to assist in evaluating the need for any additional engineering processing capacity or tuning.

CARSTxDscrdCong

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (by Service ID)
Description	Number of stack events discarded due to Routed Service congestion.
Collection Interval	30 min
Peg Condition	Stack event submitted to ComAgent by a local User Layer, and the stack event references a Routed Service that has a congestion level greater than the priority level of the stack event.
Measurement Scope	Server

Recovery

1. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screens to determine if the offered load is expected and exceeds the product's capacity.

If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.

2. It is recommended to 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

It is recommended to 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: • 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

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. It is recommended to 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.

CAStackQueueFul

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Arrayed
Description	StackEvents discarded due to ComAgent task queue full condition.
Collection Interval	30 min
Peg Condition	For each User Data egress StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent Egress Task Queue.
Measurement Scope	NE, Server

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. It is recommended to 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. It is recommended to contact *My Oracle Support (MOS)* for assistance.

CATransDscrdStaleErrRsp

Measurement Group	ComAgent Exception
Measurement Type	Simple
Measurement Dimension	Arrayed (by Service ID)
Description	Number of times that an error response was discarded because it contained a valid correlation ID value but its originating server was not the last server to which the request was sent.
Collection Interval	30 min
Peg Condition	ComAgent receives an error response stack event that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent. This measurement indicates that one or more servers are responding with errors to requests after the local ComAgent has retransmitted the requests to other destination servers. This could occur due to: • Network problems result in intermittent loss of communication between servers. • Server overload results in delayed responses
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. It is recommended to contact *My Oracle Support (MOS)* for assistance.

CATransEndAbnorm

Measurement Group	ComAgent Exception, ComAgent Performance
Measurement Type	Simple
Measurement Dimension	Arrayed (by Service ID)
Description	Number of reliable transactions that terminated abnormally.
Collection Interval	30 min
Peg Condition	• Transaction times-out waiting for a response, and the maximum number of transmits has been reached. • Transaction time-to-live limit is exceeded. • Transaction terminated due to lack of resources. **Note:** This measurement is NOT pegged for these conditions: • Transaction involves an unknown service. • Transaction involves an unregistered Routed Service.
Measurement Scope	Server

Recovery

1. Check the ComAgent Exception report to further diagnose the reasons why transactions are failing.
2. It is recommended to contact *My Oracle Support (MOS)* for assistance.

CATransEndAbnormRateAvg

Measurement Group	ComAgent Performance, ComAgent Exception
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 a sliding-metric 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 troubleshooting when compared to other measurements.
Measurement Scope	Server

Recovery

No action necessary.

CATransEndAbnormRateMax

Measurement Group	ComAgent Performance, ComAgent Exception
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 a sliding-metric 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 troubleshooting 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

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. It is recommended to 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. It is recommended to 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. It is recommended to 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. It is recommended to contact *My Oracle Support (MOS)* for assistance if needed.

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. It is recommended to 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: • 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. It is recommended to 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: • 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. It is recommended to 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: • 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. It is recommended to 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. It is recommended to 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:

- 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. It is recommended to 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

1. Use **Main Menu** > **Communication Agent** > **Configuration** > **Routed Services** screen to verify that all Routed Services expected by local applications are properly configured.
2. It is recommended to 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. It is recommended to contact *My Oracle Support (MOS)* for assistance.

OAM.ALARM measurements

Table 28: 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

Measurement Tag	Description	Collection Interval
Alarm.Minor	The number of minor alarms	5 minutes
Alarm.State	The alarm state.	5 minutes

OAM.SYSTEM measurements

Table 29: 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 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.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

Measurement Tag	Description	Collection Interval
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
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

Glossary

B

BIOS

Basic Input-Output System

Firmware on the CPU blade that is executed prior to executing an OS.

C

CAPM

Computer-aided policy making

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.

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

C

of characters signifying the end of a line of text).

D

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.

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.

Full Address Based Resolution

See FABR.

G

GLA

Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B by the Policy Diameter Routing Agent

G

(Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.

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.

HIDS

Host Intrusion Detection System

HP

Hewlett-Packard

I

IMSI

International Mobile Station Identity

A unique internal network ID identifying a mobile subscriber.

IPFE

IP Front End

A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally

I

routable IP addresses required for application clients to contact application servers.

K

KPI

Key Performance Indicator

M

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

Multi-Purpose Server

The Multi-Purpose Server provides database/reload functionality and a variety of high capacity/high speed offboard database functions for applications. The MPS resides in the General Purpose Frame.

MSISDN

Mobile Subscriber Integrated Services Digital Network [Number]

The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.

The unique, network-specific subscriber number of a mobile communications subscriber. MSISDN follows the E.164 numbering plan; that is, normally the MSISDN is the phone number that is used to reach the subscriber.

N

N

NAI

Network Access Identifier

The user identity submitted by the client during network authentication.

NPA

Number Plan Area

The North American “Area Codes.” (3 digits: 2- to-9, 0 or 1, 0-to-9. Middle digit to expand soon).

NTP

Network Time Protocol

NTP daemon

Network Time Protocol daemon – NTP process that runs in the background.

O

OAM

Operations, Administration, and Maintenance. These functions are generally managed by individual applications and not managed by a platform management application, such as PM&C.

Operations – Monitoring the environment, detecting and determining faults, and alerting administrators.

Administration – Typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning, using usage data, and maintaining system reliability.

Maintenance – Provides such functions as upgrades, fixes, new feature enablement, backup and restore tasks, and monitoring media health (for example, diagnostics).

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.

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.

S

SDS

Subscriber Database Server

Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to

S

replicate and recover provisioned data to the associated components.

SNMP

Simple Network Management Protocol.

An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.

SOAM

System Operations, Administration, and Maintenance

SOAP

Simple Object Access Protocol

SW

Software