Policy Management

Troubleshooting Guide

910-6728-001 Revision A
July 2013

Copyright 2013 Tekelec. All Rights Reserved. Printed in USA.
Legal Information can be accessed from the Main Menu of the optical disc or on the Tekelec Customer Support web site in the *Legal Information* folder of the *Product Support* tab.

Table of Contents

Chapter 1: Introduction.....22

About this Guide.....23
How This Guide Is Organized.....23
Scope and Audience.....23
Documentation Admonishments.....24
Customer Care Center.....24
Emergency Response.....26
Locate Product Documentation on the Customer Support Site.....27

Chapter 2: Incidents, Notifications, and Logs Overview.....28

About Incidents.....29
About Notifications.....29
About Logs.....29
Trace Log.....30
Syslog.....30
The SMPP Log.....30
The SMTP Log.....30
Configuring Log Settings.....30

Chapter 3: Trace Log Notifications.....33

Expanded List.....34
2 - OSSI collector establishing connection to type 34
3 - Error occurred during OSSI collector run: type 34
4 - Starting OSSI collector run.....34
5 - OSSI collector run completed.....35
6 - OSSI collector run aborted.....35
7 - OSSI collector error reading configuration file: file-name 35
8 - OSSI collector established connection.....36
9 - OSSI collector could not establish connection host port 36
12 - OSSI collector did not find configuration parameter: parameter-name 3 6
13 - Error validating field 37
14 - Data Collector started.....37
21 - Starting Subnet SNMP Collector task.....37

22 - SNMP timeout while collecting Subnet data from CMTS name 38
23 - SNMP error type while collecting Subnet data from CMTS name 38
24 - Skipping Subnet collection from CMTS name because the SNMP community string is empty.....38
38 - Subnet SNMP Collector Task Status CMTSs.....39
39 - Finishing Subnet SNMP Collector task.....39
41 - Starting Service Class SNMP Collector task.....39
42 - SNMP timeout while collecting Service Class data from CMTS name 4 0
43 - SNMP error type while collecting Service Class data from CMTS name 4 0
44 - Skipping Service Class collection from CMTS name because the SNMP community string is empty.....41
58 - Service Class SNMP Collector Task Status.....41
59 - Finishing Service Class SNMP Collector task.....41
61 - Starting Subscriber SNMP Collector task.....42
62 - SNMP timeout while collecting Subscriber data from CMTS name 4 2
63 - SNMP error type while collecting Subscriber data from CMTS name 4 2
64 - Invalid cable modem MAC addraess MAC-address retrieved from CMTS name 43
65 - Invalid cable modem IP address ip-address for MAC MAC-address retrieved from CMTS name 43
66 - Invalid CPE IP address ip-address behind cable modem MAC-address retrieved from CMTS name 43
68 - Skipping Subscriber collection from CMS name because the SNMP community string is empty.....44
78 - Subscriber SNMP Collector Task Status.....44
79 - Finishing Subscriber SNMP Collector task.....45
81 - Starting CMTS Distributor task.....45
82 - Error while sending CMTS data to Policy Server: name 45
98 - CMTS Distributor Task Status Policy Server.....46
99 - Finishing CMTS Distributor task.....46
101 - Starting Subscriber Distributor task.....46
102 - Error while deleting Subscriber data from Policy Server: name 47
103 - Error while updating CMTS data on Policy Server: name 47
104 - Error while sending Reconfigure message to Policy Server: name 4 7
105 - Error while sending Refresh Channels message to Policy Server: name 48

106 - Error while sending Refresh Accounts message to Policy Server: name 48
107 - Error while sending Tier data to Policy Server: name 48
108 - Error while sending Channel data to Policy Server: name 49
118 - Subscriber Distributor Task Status....49
119 - Finishing Subscriber Distributor task....49
121 - Starting OSSI Distributor task....50
122 - Error occurred during OSSI distributor run: type 50
123 - OSSI distributor run aborted....50
124 - Error connection to Remote MA: host-name 51
125 - Error updating Accounts to remote MA:host-name 51
126 - Error updating CMTSs to remote MA: host-name 51
127 - Error updating Tiers to remote MA: host-name 52
128 - Error updating Entitlements to remote MA: host-name 52
139 - Finishing OSSI Distributor task....52
141 - Starting CMTS MA Collector task....53
142 - Error while collecting CMTS data from Management Agent: name 5 3
157 - CMTS MA Collector task status....53
158 - CMTS MA Collector Task Status....54
159 - Finishing CMTS MA Collector Task....54
161 - Starting Pcmm Routing Distribution task....54
177 - PCMM Distribution Task Status....55
178 - PCMM Distribution Task Status....55
179 - Finishing PCMM Routing Distribution task....55
180 - Task task - name was run manually....56
201 - Start Healthchecker task....56
219 - Finishing Healthchecker task....56
220 - Starting AlertAging task....57
239 - Finishing AlertAging task....57
241 - OM Statistics collection complete and data is available for request....57
276 - Statistics Rsync Cleanup task completed successfully....58
278 - Statistics Rsync Cleanup Task failed....58
279 - Finished Statistics Rsync Cleanup Task....58
401 - Starting Stats Files Generator Task....59
402 - Stats Files Generator Task completed successfully....59
403 - Stats Files Generator Task failed #1, 2, 3, or 4....59
404 - Finishing Stats Files Generator Task....60
406 - Sync utility failed to sync stats files to mates. Reason: reason 60
407 - Stats Files Generator Task has removed some files which were not synced to remote servers (…)....61

501 - Starting Stats Files Synchronization # 1, 2, 3, or 4.....61
502 - Stats Files Synchronization #1, 2, 3, or 4 completed successfully.....61
503 - Stats Files Synchronization # 1, 2, 3, or 4: Task Failure(s) - failure messages.....62
504 - Finishing Stats Files Synchronization # 1, 2, 3, or 4.....62
505 - The Local Repository does not exist, you need to check whether Stats Files Generator Task was executed successfully or not.....62
506 - Stats Files Synchronization #1, 2, 3, or 4: Task still failed for sync local repository to remote server (xxx.xxx.xxx.xxx) after retry 3 times.....63
507 - Stats Files Synchronization #1, 2, 3, or 4: Task was successful for sync local repository to remote server (xxx.xxx.xxx.xxx) after retry 2 times.....63
1004 - PCMM: Lost connection with AM id 64
1010 - PCMM: Received msg-type from AM id 64
1011 - PCMM: Sending msg-type to id 64
1012 - PCMM: Received msg-type from id 65
1013 - PCMM: Sending msg-type to AM id 65
1014 - PCMM: Failed (num attempts) to send msg-type event message to id 66
1015 - PCMM: Successfully sent msg-type event message to id 66
1016 - PCMM: Failover initiated for RKS id, reverting to id 66
1017 - Failed (TOO BUSY) to send msg-type event message to id 67
1020 - PCMM: Rejecting msg-type - no PEP available for SubID IP; trap will be sent to NM.....67
1021 - PCMM: Rejecting msg-type - invalid gate ID gateid 68
1022 - PCMM: Rejecting msg-type - AMID mismatch - request msg-amid doesn't match gate MPE-AMID.....68
1023 - PCMM: Rejecting msg-type - SubId mismatch - request msg-id doesn't match gate mpe-id 69
1024 - PCMM: Rejecting msg-type - Unrecognized Subscriber id 69
1025 - PCMM: Rejecting msg-type - Unauthorized AmID id 70
1026 - PCMM: Rejecting msg-type - Unrecognized Service Class Name name 70
1027 - PCMM: Rejecting msg-type - Incompatible Envelopes -env-type ENV exceeds env-type ENV.....71
1028 - PCMM: Rejecting msg-type - Classifier count exceeds CMTS limit.....71
1029 - PCMM: Rejecting msg-type - I/O Error while sending to id 72
1101 - DQOS: Established connection to id 72
1102 - DQOS: Lost connection to id 72
1104 - DQOS: Lost connection with CMS id 73
1110 - DQOS: Received msg-type from CMS id 73
1111 - DQOS: Sending msg-type to id 73

1112 - DQOS: Received msg-type from id msg-contents 74
1113 - DQOS: Sending msg-type to CMS id 74
1120 - DQOS: Rejecting msg-type - no CMTS available for SubID id 74
1121 - DQOS: Rejecting msg-type - invalid gate id id 75
1123 - DQOS: Rejecting msg-type - SubId mismatch - request msg-id doesn't match gate mpe-id 75
1124 - DQOS: Rejecting msg-type - Unrecognized Subscriber id 76
1129 - DQOS: Rejecting msg-type - DQOS I/O Error while sending to id 7 6
1150 - DQOS: Rejecting msg-type - Rejected by policy name.....76
1204 - SPC DQOS: Lost connection with CMS id 77
1209 - SPC DQOS: Deleting gate gateid, T1 Timer expired.....77
1210 - SPC DQOS: Received msg-type from CMS id msg-contents 77
1213 - SPC DQOS: Sending msg-type to CMSid 78
1221 - SPC DQOS: Rejecting msg-type - invalid global session id globalsessionid 78
1231 - SPC DQOS: Rejecting msg-type - invalid ingress id ingressid 79
1232 - SPC DQOS: Rejecting msg-type - no path to root zone for ingress id ingressid 79
1233 - SPC DQOS: Dropping msg-type - invalid gate id gateid 79
1314 - NAC: Abnormal delete of session.....80
1315 - NAC: Normal delete of session.....80
1316 - NAC: Allowed session.....81
1320 - NAC: Rejecting msg-type - no path available from SUB-IP to SERVER-IP 81
1321 - NAC: Rejecting msg-type - subscriber with address SUB-IP is unknown (session ID VoD-ID).....81
1322 - NAC: Allowing msg-type - subscriber with unknown address SUB-IP (session ID VoD-ID).....82
1323 - NAC: No account information for subscriber SUB-IP (session ID VoD-ID).....82
1324 - NAC: Subscriber with address SUB-IP is unknown (session ID VoD-ID).....83
1351 - NAC: Both static and dynamic definitions for subscriber IP address SUB-IP, using dynamic definition.....83
1352 - NAC: Could not find BRAS endpoint endpoint in path path - rejecting.....83
1370 - BRAS: COPS-PR declared an IP address (ip) already defined as static in account account 84
1401 - Diameter: Transport connection opened with peer peer_id 84
1402 - Diameter: Transport connection closed with the peer 0 84

1403 - Diameter: Transport connection disconnected by the peer 0 85
1404 - Diameter: Sent msg to peer peer_id connection conn_ id 85
1405 - Diameter: Received msg from peer peer_id connection conn_id
.....8 6
1406 - Diameter: Error processing message msg from peer peer_id
connection conn_id 86
1407 - Diameter: Peer id (connection_id) status changed from
previous_status to new_status 86
1408 - Diameter: New connection rejected.....87
1409 - Diameter: Rejecting msg_type from peer_id - con_id AVP(s) not
found in request request_details 87
1410 - Diameter: Response timeout for msg_type sent to conn_id
msg_details 88
1411 - Diameter: Received Duplicate message msg_type from conn_id
msg_details 88
1412 - Diameter: Sent {type} to {destination} in {connection ID} mes
{message} 88
1413 - Diameter: Received {type} from {sender} in {connection ID} mes
{message} 89
1414 - Diameter: SCTP path on association ID address
ADDR_CONFIRMED/ADDR_UNREACHABLE/ADDR_AVAILABLE.....89
1420 - Diameter: Rejecting application_request - no PCEF available for
subscriber.....89
1421 - Diameter: No default QoS profile defined for media type 90
1440 - Diameter: Rejecting request for subscriber sub_id - No Network
Element found for node node_id 90
1441 - Diameter: PCC rule rule failed for subscriber sub_id xxx - Rule
failure code code 91
1442 - Diameter: PCC rule rule retry x of y for subscriber sub_id xxx. Next
retry in z seconds.....91
1443 - Diameter: PCC rule rule retry failed after n attempts for subscriber
sub_id xxx 91
1444 - Diameter: PCC rule rule retry canceled for subscriber sub_id xxx
.....9 2
1445 - Diameter: PCC rule rule retry aborted for subscriber sub_id xxx -
Too many retries in progress (n attempts).....92
1446 - Diameter: The maximum number of PDN connections has been
exceeded for subscriber ID 92
1450 - SceGX: No SCE Profile or Default Profile set for subscriber
subscriber 93
1470 - Begin diameter session binding cleanup task.....93

1471 - End of database iterations....94
1472 - End of diameter session binding cleanup task....94
1600 - DBPLUGIN: No matches for criteria, search type ID 94
1601 - LDAP: Established Connection to srv 95
1602 - LDAP: Closing conection to srv 95
1605 - LDAP: Attempted connection to 0 failed, reason: 1 95
1610 - LDAP: Search failure for ID due to the following error: error message 96
1611 - LDAP: Searching for stype: criteria 96
1612 - LDAP: Search results for stype filter are results 96
1613 - LDAP: No matches for stype filter 97
1614 - LDAP: Multiple matches for stype filter 97
1615 - LDAP: Unexpected search failure for stype filter, reason: msg 97
1617 - LDAP: Detailed description of LDAP modification to be initiated....98
1619 - LDAP: Unexpected modify failure for process ID key, reason: message 98
1620 - LDAP: Operation queue process ID in distress. Queue capacity exceeds event message....98
1621 - LDAP: Operation queue process ID has cleared and is no longer in distress. Capacity is below event message 99
1622 - LDAP:Operation queue process ID is currently at 100% and will begin rejecting new LDAP Modify requests....99
1623 - LDAP:Modify failure. Unable to modify fields at distinguished name due to the following error: message 99
1624 - LDAP:Modify failure. Unable to perform modify due to the following error: message 100
1626 - LDAP:Update unsuccessful: message 100
1661 - SH:Peer Realm detailed message 100
1662 - SH:Bad primary/secondary address reason 101
1663 - SH:Searching for peer ID: query 101
1664 - SH:Search results for query peer ID are: error message 101
1665 - SH:No matches for peer ID query 102
1666 - SH:Unexpected search failure on peer ID 102
1667 - SH:Subscribing for sub type name: element 102
1668 - SH:Subscription results for user ID type element are: response 103
1669 - SH:Unexpected subscription failure for user ID type element, reason: response 103
1670 - SH:Unsubscribing for sub type name: element 103
1671 - SH:Unsubscription results user ID type element are: response 104
1672 - SH:Unexpected unsubscription failure user ID type element are: response 104

1673 - SH:Received notification: results 104
1681 - MSR: Established connection to ip:port 105
1682 - MSR: Closing Connection to ip:port 105
1683 - MSR: Connection to the MSR server at the specified IP address was closed unexpectedly.....105
1684 - MSR: Closing a secondary MSR connection to revery to a primary connection.....106
1685 - MSR: Connection attempt to MSR server failed.....106
1686 - MSR: Searching for type: key 107
1687 - MSR: Searching for type: key 107
1690 - MSR: Unexpected search failure for type key, reason: msg 107
1691 - MSR: Updating type: key 108
1692 - MSR: Update result for type key are: result 108
1693 - MSR: Unexpected update failure for type key, reason: msg 108
1694 - MSR: Subscribing for type: key 109
1695 - MSR: Subscription results for type key are: results 109
1696 - MSR: Unexpected subscription fialure for type key, reason: msg 109
1697 - MSR: Unsubscribing for type: key 110
1698 - MSR: Unsubscription results for type key are: result 110
1699 - MSR: Unexpected unsubscription failure for type key, reason: msg 110
1701 - COPS-PR: Connection accepted from gateway IP ip-address, port port 111
1702 - COPS-PR: Lost connection with gateway id 111
1703 - COPS-PR: Rejecting OPN message from id. Unknown gateway.....111
1711 - COPS-PR: Received msg-type from id 112
1712 - COPS-PR: Sending msg-type to id 112
1721 - COPS-PR: Dropping msg-type from id - reason 113
1740 - BRAS: Transmit buffer for n extended from x to y 113
1741 - BRAS: Transmit buffer for id shrunk from x to y 113
1750 - Gx-Plus: Received CCR-I, session ID x subid y from id 114
1751 - Gx-Plus: Received CCR-T, session ID x from id 114
1756 - Gx-Plus: Learnt new endpoint id, x from gateway y 114
1763 - Gx-Plus: Start state synchronization with gateway id 115
1764 - Gx-Plus: State synchronization with gateway id has completed.....115
1765 - Gx-Plus: Drop all the bras endpoints and diameter sessions because of cold reboot from gateway id 116
1766 - Gx-Plus: Deleting endpoint n, x due to CCR-T from gateway id 116
1767 - Gx-Plus: Deleting stale entry for IP n, x from gateway id 116

1768 - Gx-Plus: Received warm reboot message from gateway id 117
1769 - Gx-Plus: Received AYT message from gateway id 117
2300 - TOD: Time period(s) changed from prev_time_periods to new_time_periods 117
2301 - TOD: Transition to time period(s) new_time_periods started.....118
2302 - TOD: Transition to time period(s) new_time_periods was still in progress when time periods changed. transition aborted.....118
2303 - TOD: Transition to time period(s) new_time_periods successfully completed.....119
2304 - TOD: Transition to time period(s) new_time_periods failed to complete normally.....119
2305 - TOD: Transition to time period(s) new_time_periods was aborted.....119
2306 - TOD:Transition to time period(s) current time periods was invoked by the operator.....120
2500 - SCE:Connecting to SCE ID 120
2501 - SCE:Lost connection to SCE ID 120
2502 - SCE:Received request type for subscriber sub ID from SCE ID 121
2503 - SCE:Sent request type for subscriber sub ID and package package ID to SCE ID 121
2504 - SCE:Sent Logout request for subscriber sub ID to SCE ID 121
2505 - SCE:Received error error message for operation name setting package package for subscriber sub ID from SCE ID 122
2506 - SCE:Error detailed message when processing request type from subscriber ID 122
2507 - SCE:Re-setting package from previous package ID to new package ID for subscriber subscribe ID at SCE ID 122
2549 - SMS:SMSR internal queue is full: queue name.....123
2550 - SMS:SMS Relay is not enabled to receive message. optional additional details 123
2551 - SMS:Configured SMS Relay endpoint: SMS end point 123
2552 - SMS:Sent to id: ID using SMS Relay defined at end point\n Message:message 124
2553 - SMS:Unable to send SMS to ID. Invalid Billing Day billing day configured.....124
2555 - SMS:Error sending SMS to ID using SMS Relay defined at end point\n Message:message 124
2556 - SMS:Unable to send SMS to response message using SMS Relay defined at end point ID 125
2557 - SMS:Unable to send SMS to user ID. User's MSISDN could not be found.....125
2565 - SMTP:Connection has been closed to MTA IP Address 125

2566 - SMTP:Connection established to MTA IP Address 126
2567 - SMTP:Error attempting to establish a new connection to mta\n Error:error 126
2611 - MSR: Received notification: msg 126
2700 - New DRA binding created.....127
2701 - RADIUS:Initializing communications on port port number 127
2701 - DRA binding released between subscriber and MPE device.....127
2702 - Existing binding found.....128
2703 - RADIUS:Start failed on port port number 128
2703 - MRA did not find binding information for subscriber.....128
2704 - RADIUS:Received message code / status type:accounting type pocket ID / session ID from client address.message 129
2704 - Binding Release Task STARTED | COMPLETED | ABORTED 129
2705 - RADIUS:Dropping invalid message request. reason 129
2705 - Duplicate bindings have been detected for list_of_user_ids on list_of_MRAs 130
2706 - RADIUS:Dropping message with bad MD5, probably bad password in request 130
2706 - Binding cleanup task has been started.....130
2707 - RADIUS:Sent message code [accounting status type / pocket ID] to session ID.message 131
2707 - Binding cleanup task is finished and processed 0 stale bindings, 1 duplicate bindings, and 2 stale sessions.....131
2710 - RADIUS:Stopping communication for port number 132
2900 - ADMISSION: System is in busy state because resource name: criteria admission criteria 132
2901 - ADMISSION: System is in normal state.....132
2902 - ADMISSION: Monitored resource resource-name is in busy state: criteria threshold 133
2903 - ADMISSION: Monitored resource resource-name is in normal state: criteria threshold 133
2904 - Diameter/RADIUS protocol is in a busy state.....133
2905 - Diameter/RADIUS protocol is in a normal state.....134
3100 - Certificate x expires in n days 134
3101 - Certificate x has expired.....134
4000 - Policy Action generated critical alarm.....135
4001 - Policy Action generated major alarm.....135
4002 - Policy Action generated minor alarm.....136
4003 - CAC: Exception while recreating Tandberg session.....136
4004 - CAC: Recreating Tandberg session id due to synch operation with url 136

4005 - CAC: Failed to recreate Tandberg session id due to sync with url 137
4065 - CAC: Exception while reading local session ID list....137
4066 - CAC: Failed to create CAC session ID id 137
4068 - CAC: Exception while sync operation terminated CAC session ID id 138
4070 - CAC: Failed to release resources for session ID id 138
4080 - CAC: Error locating session in CAC database: error-message 138
4096 - CAC: Created CAC session ID id due to request from VoD server at server-ip 139
4144 - CAC: Exception while reserving resources for id: error-message 139
4154 - CAC: This blade is now active....139
4155 - CAC: This blade is now inactive. Canceling any synchronization in progress....140
4156 - CAC: Unknown response from gate delete request....140
4164 - CAC: Starting synchronization with server-url 140
4165 - CAC: Synchronization with server-url complete....141
4172 - CAC: Locally removing session id due to synchronization mismatch with Seachange/Tandberg server at ip-address 141
4173 - CAC: Locally removing session id due to synchronization timeout with Seachange/Tandberg server at ip-address 141
4175 - CAC: Requesting removal of session id from Seachange/Tandberg server at ip-address due to synchronization mismatch....142
4177 - CAC: Rejecting create of session ID id from server at ip-address: duplicate session....142
4178 - CAC: Tandberg session ID id missing in session list on Tandberg server. Issuing specific query to url 143
4179 - CAC: Tandberg session ID id still missing in session list on Tandberg server at url - scheduling removal....143
4180 - CAC: Keepalive status request from Tandberg server at ip-address 143
4181 - CAC: Session list status request from Seachange/Tandberg server at ip-address 144
4182 - CAC: Session detail status request from Tandberg server at ip-address for session ID id 144
4183 - CAC: Version status request from Tandberg server at ip-address 144
4184 - CAC: Seachange/Tandberg reserve of session id on ip-address complete....145
4185 - CAC: Seachange/Tandberg release of session id complete....145

4188 - CAC: No keepalive response from Tandberg server at url 145
4189 - CAC: Exception while releasing session id from Tandberg server.....146
4190 - CAC: Tandberg server requesting release of session ID id 146
4191 - CAC: No version status response from Tandberg server at url 146
4192 - CAC: Version report from Tandberg server at url 147
4193 - CAC: Invalid version report from Tandberg server at url 147
4194 - CAC: Sending keepalive request to Tandberg server at url 147
4195 - CAC: Received keepalive response from Tandberg server at url 148
4196 - CAC: Sync mismatch with Seachange/Tandberg server at ip-address: VoD server has n sessions missing on MPE.....148
4200 - CAC: Failed to create CAC session ID id from VoD Server at server-ip for subscriber IP sub-ip: status 148
4201 - CAC: Exception while Seachange/Tandberg sync operation with url terminated CAC session ID id 149
4203 - CAC: Error requesting session list from Seachange/Tandberg server at url 149
4205 - CAC: Starting synchronization with Seachange/Tandberg server at url 150
4206 - CAC: Synchronization with Seachange/Tandberg server at url complete.....150
4207 - CAC: Max sync failures with Seachange/Tandberg server at ip-address: removing n sessions.....150
4208 - CAC: Seachange/Tandberg reserve of duplicate session id on ip-address complete: status status, duration time ms.....151
4300 - RC ip-address Unreachable.....151
4301 - RC ip-address Reachable.....151
4302 - RC ip-address Unreachable - operation: operation 152
4550 - Policy Trace name: message 152
4551 - Policy Trace name: message 152
4552 - Policy Trace name: message 153
4560 - Policy Action Trace: message 153
4561 - Policy Action Trace: message 153
4562 - Policy Action Trace: message 154
4563 - Policy Action Trace: message 154
4564 - Policy Action Trace: message 154
4565 - Policy Action Trace: message 155
4566 - Policy Action Trace: message 155
4567 - Policy Action Trace: message 155
4600 - MPE or MRA rejects a secondary connection.....156

4601 - MPE or MRA reverts from a secondary connection to a primary connection....156
4602 - More than one server in a cluster is Active at a time....157
4603 - Max primary site failure threshold reached....157
4604 - Policy Cluster Offline Failure....157
4610 - Sh Connections operation Successful for MPEs' name, Failed for MPEs' name....158
4700 - Upgrade Manager command return message: message....158
10000 - ADS: Analytics Data Stream connection to Analytics Client ID has been established for Channel: Channel Type, ex Policy Event Version: ADS Interface Version Connection established to the MPE from an Analytics client....159
10001 - ADS: Analytics Data Stream connection to Analytics Client ID was closed....159
10002 - ADS: Lost Analytics Data Stream connection to Analytics Client ID....159
10003 - ADS: Error processing Analytics Data Stream message received from Analytics Client ID....160
10004 - ADS: Error sending Analytics Data Stream message to Analytics Client ID....160
10005 - ADS: Analytics Data Stream encountered an error....160
10006 - SY: Received notification from Sy Identity message: Diameter message....161
10007 - SY: Peer Realm is undefined....161
10008 - SY: Primary address is undefined....161
10009 - SY: Searching Sy Identity for subscriber: Subscriber IDs....162
10010 - SY: Search results from peer Sy Identity for subscriber Subscriber IDs are: Policy Counter values....162
10012 - SY: Search failure on Sy Identity: Diameter Error Code subscriber Subscriber IDs....162

Chapter 4: Alarms and Events....164

Alarms formatting information....165
Alarm and Event Severity Levels....165
Platform (31000-32700)....165
31000 - S/W Fault....165
31001 - S/W Status....166
31002 - Process Watchdog Failure....166
31003 - Thread Watchdog Failure....166
31100 - DB Replication Fault....166

31101 - DB Replication To Slave Failure....167
31102 - DB Replication From Master Failure....167
31103 - DB Replication Update Fault....167
31104 - DB Replication Latency Over Threshold....168
31105 - DB Merge Fault....168
31106 - DB Merge To Parent Failure....168
31107 - DB Merge From Child Failure....168
31108 - DB Merge Latency Over Threshold....169
31109 - Topology Config Error....169
31110 - DB Audit Fault....169
31111 - DB Merge Audit in Progress....170
31112 - DB Replication Update Log Transfer Timed Out....170
31113 - DB Replication Manually Disabled....170
31114 - DB Replication over SOAP has failed....170
31115 - DB Service Fault....171
31116 - Excessive Shared Memory....171
31117 - Low Disk Free....171
31118 - DB Disk Store Fault....171
31119 - DB Updatelog Overrun....172
31120 - DB Updatelog Write Fault....172
31121 - Low Disk Free Early Warning....172
31122 - Excessive Shared Memory Early Warning....172
31123 - DB Replication Audit Complete....173
31124 - DB Replication Audit Command Error....173
31125 - DB Durability Degraded....173
31126 - Audit Blocked....173
31130 - Network Health Warning....174
31140 - DB Perl Fault....174
31145 - DB SQL Fault....174
31146 - DB Mastership Fault....174
31147 - DB UpSyncLog Overrun....175
31148 - DB Lock Error Detected....175
31200 - Process Management Fault....175
31201 - Process Not Running....175
31202 - Unkillable Zombie Process....176
31206 - Process Mgmt Monitoring Fault....176
31207 - Process Resource Monitoring Fault....176
31208 - IP Port Server Fault....176
31209 - Hostname Lookup Failed....177
31213 - Process Scheduler Fault....177
31214 - Scheduled Process Fault....177

31215 - Process Resources Exceeded....177
31216 - SysMetric Configuration Error....178
31220 - HA Config Monitor Fault....178
31221 - HA Alarm Monitor Fault....178
31222 - HA Not Configured....178
31223 - HA Heartbeat Transmit Failure....179
31224 - HA Configuration Error....179
31225 - HA Service Start Failure....179
31226 - HA Availability Status Degraded....179
31227 - HA Availability Status Failed....180
31228 - HA Standby Server Offline....180
31229 - HA Score Changed....180
31230 - Recent Alarm Processing Fault....181
31231 - Platform Alarm Agent Fault....181
31232 - HA Late Heartbeat Warning....181
31240 - Measurements Collection Fault....181
31250 - RE Port Mapping Fault....182
31260 - DB SNMP Agent....182
31270 - Logging Output....182
31280 - HA Active to Standby Transition....182
31281 - HA Standby to Active Transition....183
31282 - HA Management Fault....183
31283 - HA Server Offline....183
31284 - HA Remote Subscriber Heartbeat Warning....183
31290 - HA Process Status....184
31291 - HA Election Status....184
31292 - HA Policy Status....184
31293 - HA Resource Link Status....185
31294 - HA Resource Status....185
31295 - HA Action Status....185
31296 - HA Monitor Status....185
31297 - HA Resource Agent Info....186
31298 - HA Resource Agent Detail....186
32113 - Uncorrectable ECC Memory Error....186
32114 - SNMP Get Failure....186
32300 – Server Fan Failure....187
32301 - Server Internal Disk Error....187
32302 – Server RAID Disk Error....187
32303 - Server Platform Error....188
32304 - Server File System Error....188
32305 - Server Platform Process Error....188

32307 - Server Swap Space Shortage Error....188
32308 - Server Provisioning Network Error....189
32312 - Server Disk Space Shortage Error....189
32313 - Server Default Route Network Error....189
32314 - Server Temperature Error....190
32315 – Server Mainboard Voltage Error....190
32316 – Server Power Feed Error....191
32317 - Server Disk Health Test Error....191
32318 - Server Disk Unavailable Error....192
32320 – Device Interface Error....192
32321 – Correctable ECC memory error....192
32322 – Power Supply A error....192
32323 – Power Supply B Error....193
32324 – Breaker panel Feed Error....193
32325 – Breaker Panel Breaker Error....193
32326 – Breaker Panel Monitoring Error....194
32327 – Server HA Keepalive Error....195
32331 – HP disk problem....195
32332 – HP Smart Array controller problem....195
32333 – HP hpacucliStatus utility problem....196
32335 - Switch Link Down Error....196
32336 – Half open socket limit....196
32500 – Server Disk Space Shortage Warning....197
32501 – Server Application Process Error....197
32502 – Server Hardware Configuration Error....197
32505 – Server Swap Space Shortage Warning....197
32506 – Server Default Router not Defined....198
32507 – Server Temperature Warning....198
32508 – Server Core File Detected....199
32509 – Server NTP Daemon Not Synchronized....199
32510 – CMOS Battery Voltage Low....199
32511 – Server Disk Self Test Warning....199
32512 – Device Warning....200
32513 – Device Interface Warning....200
32514 – Server Reboot Watchdog Initiated....200
32515 – Server HA Failover Inhibited....200
32516 – Server HA Active To Standby Transition....201
32517 – Server HA Standby To Active Transition....201
32518 – Platform Health Check Failure....201
32519 – NTP Offset Check Failure....202
32520 – NTP Stratum Check Failure....202

32521 – SAS Presence Sensor Missing....202
32522 – SAS Drive Missing....202
32524 – HP disk resync....203
32525 – Telco Fan Warning....203
32526 – Telco Temperature Warning....203
32527 – Telco Power Supply Warning....204
32528 – Invalid BIOS value....204
32529 – Server Kernel Dump File Detected....204
32530 – TPD Upgrade Fail Detected....204
32531 – Half Open Socket Warning....205
32532 – Server Upgrade Pending Accept/Reject....205
QBus Platform (70000-70999)....205
70001 - QP_procmgr failed....205
70002 - QP Critical process failed....206
70003 - QP Non-critical process failed....206
70004 - QP Processes down for maintenance....206
70010 - QP Failed Server-backup Remote Archive Rsync....207
Error Code Details for Alarms 70010 and 70011....207
70011 - QP Failed System-backup Remote Archive Rsync....208
70012 - QP Failed To Create Server Backup....209
70013 - QP Failed To Create System Backup....209
70015 - VIP Route Add Failed....209
70020 - QP Master database is outdated....210
70021 - QP slave database is unconnected to the master....210
70022 - QP Slave database failed to synchronize....211
70023 - QP Slave database lagging the master....211
70024 - QP Slave database is prevented from synchronizing with the master....212
70025 - QP Slave database is a different version than the master....212
70026 - QP Server Symantec NetBackup Operation in Progress....212
Policy Server (71000-89999)....213
71004 - AM CONN LOST....213
71101 - DQOS DOWNSTREAM CONNECTION CLOSED....213
71102 - MSC CONN LOST....214
71104 - DQOS AM CONNECTION CLOSED....214
71204 - SPC CONN CLOSED....214
71402 - TRANSPORT CLOSED....215
71403 - TRANSPORT DISCONNECTED....215
71408 - DIAMETER NEW CONN REJECTED....216
71414 - SCTP PATH STATUS CHANGED....216
71605 - LDAP CONN FAILED....217

71630 - DHCP UNEXPECTED EVENT ID....217
71631 - DHCP UNABLE TO BIND EVENT ID....217
71632 - DHCP RESPONSE TIMEOUT EVENT ID....218
71633 - BAD RELAY ADDRESS EVENT ID....218
71634 - DHCP BAD PRIMARY ADDRESS EVENT ID....218
71635 - DHCP BAD SECONDARY ADDRESS_EVENT ID....219
71684 - SPR CONNECTION CLOSED....219
71685 - MSR DB NOT REACHABLE....219
71702 - BRAS CONNECTION CLOSED....220
71703 - COPS UNKNOWN GATEWAY....220
71801 - PCMM NO PCEF....221
71805 - PCMM NOCONNECTION PCEF....221
72198 - SMSR SMSC SWITCHED TO PRIMARY....221
72199 - SMSR SMSC SWITCHED TO SECONDARY....222
72210 - PCMM REACHED MAX GATES EVENT ID....222
72211 - PCMM REACHED MAX GPI EVENT ID....222
72501 - SCE CONNECTION LOST....223
72549 - SMSR QUEUE FULL....223
72559 - SMSR SMSC CONN CLOSED....223
72565 - SMSR SMTP CONN CLOSED....224
72703 - RADIUS SERVER START FAILED....224
72706 - RADIUS SERVER CORRUPT AUTH....224
72904 - DIAMETER TOO BUSY....225
72905 - RADIUS TOO BUSY....225
74000 - POLICY CRITICAL ALARM....225
74001 - POLICY MAJOR ALARM....226
74002 - POLICY MINOR ALARM....226
74020 - DELETE EXPIRE FILES....226
74021 - FILE SYNCHRONIZATION FAILURE....227
74602 - QP Multiple Active In Cluster Failure....227
74603 - QP Max Primary Cluster Failure Threshold....228
74604 - QP Policy Cluster Offline Failure....228
75000 - POLICY LIBRARY LOADING FAILED....229
78000 - ADS CONNECTION LOST....229
78001 - RSYNC FAILED....229
80001 - QP DB State Transition....230
80002 - QP MySQL Relay Log Dropped....230
80003 - QP MySQL Database Level Advertisement....231
82704 - BINDING RELEASE TASK....231
84004 - POLICY INFO EVENT....232
86001 - APPLICATION IS READY....232

86100 - CMP USER LOGIN....232
86101 - CMP USER LOGIN FAILED....233
86102 - CMP USER LOGOUT....233
86200 - CMP USER PROMOTED SERVER....233
86201 - CMP USER DEMOTED SERVER....234
86300 - SH ENABLE FAILED....234
86301 - SH DISABLE FAILED....234
Glossary....236

List of Tables

Table 1: Admonishments.....24
Table 2: Error Code and Meaning - Alarms 70010/70011.....207

Chapter 1

Introduction

Topics:

- *About this Guide.....23*
- *How This Guide Is Organized.....23*
- *Scope and Audience.....23*
- *Documentation Admonishments.....24*
- *Customer Care Center.....24*
- *Emergency Response.....26*
- *Locate Product Documentation on the Customer Support Site.....27*

Introduction provides a content overview of this guide with a brief summary about incidents, notifications, and the ID ranges for alarms and events. It also includes Tekelec contact information and how to locate product documentation on the Tekelec Customer Support site.

About this Guide

The *Policy Management Troubleshooting Guide* compiles all available notifications, including any alarms or events generated by the system or a Policy action. Alarms alert an operator to action, while events provide information about an expected incident and can be used for debugging purposes. These notifications are sent from different areas of the Policy Management system and are stored for active viewing or historical purposes.

The *Policy Management Troubleshooting Guide* provides all available notifications that do not generate an alarm. Notifications use a 3-, 4-, or 5-digit ID, such as 401, 1683, or 10001.

Alarms and events are grouped under an ID range, which is associated with the type of alarm or event:

- 31000 - 32700 Tekelec Platform
- 70000 - 70999 QBus Platform (QP)
- 71000 - 89999 Policy Server

How This Guide Is Organized

The information in this guide is presented in the following order:

- *Introduction*
- *Incidents, Notifications, and Logs Overview*
  - *About Incidents*
  - *About Notifications*
  - *About Logs*
- *Trace Log Notifications*
- *Alarms and Events*
  - *Alarms formatting information*
  - *Alarm and Event Severity Levels*
  - *Platform (31000-32700)*
  - *QBus Platform (70000-70999)*
  - *Policy Server (71000-89999)*

Scope and Audience

This guide is intended for trained and qualified system operators and administrators who are responsible for managing a Policy Management system.

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

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

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

    001-888-367-8552

  - **Peru**

    Phone:

    0800-53-087

  - **Puerto Rico**

    Phone:

    1-888-367-8552 (1-888-FOR-TKLC)

  - **Venezuela**

    Phone:

0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

Incidents, Notifications, and Logs Overview

Topics:

- *About Incidents.....29*
- *About Notifications.....29*
- *About Logs.....29*

An incident is an occurrence in the system that was triggered by the system or a policy action. An incident sends a notification, which is a message about the incident, to a log so it can be tracked and stored to be viewed by the operator.

Incidents, Notifications, and Logs Overview describes the concepts of incidents, notifications, and logs, and provides a procedure for configuring log settings.

About Incidents

There are two types of incidents:

- **System incident**: an occurrence in the system, such as establishing a connection to a remote server. The system incident is further divided into platform-level and application-level incidents. Platform-level system incidents send alarms and events; application-level system incidents send trace log notifications, and in some cases, alarms and events.
- **Policy Action incident**: Occurs when an operator uses policy actions to generate notifications based on policy execution. Policy Action incidents can send trace log notifications, syslog notifications, and alarms and events.

The incident definition contains details about all notifications, such as trace log severity, message text, and alarm/event information.

Incidents can generate notifications. An example incident is "establishing a connection to a remote server." Some incidents can generate more than one type of notification -- for example, a trace log notification and an alarm. The ID indicates the source of the alarm or event as shown in the ID ranges below:

- 31000 - 32700 Tekelec Platform alarms and events
- 70000 - 70999 QBus Platform (QP) alarms and events
- 71000 - 79999 Policy Server alarms
- 80000 - 89999 Policy Server events

About Notifications

A notification is a message sent by an incident. There are various logging mechanisms that receive these notifications, as well as an alarm system to notify operators of issues that may need action. Notifications may generate a trace log, syslog, and/or an alarm or event.

About Logs

Log files receive various types of notifications and log them for historical purposes.

There are several types of logs:

- Trace Log
- Syslog
- SMPP Log
- SMTP Log

Trace Log

The Trace Log is an application-level system notification used to trace and debug application-level incidents, and is available on the Logs tab of the Policy Server Configuration (Administration) page and the MRA Configuration (Administration) page. The Trace Log page displays:

- General application notifications
- Policy Application notifications
- Policy server notifications
- Policy action notifications that generate Trace Log entries

The log entries provide an incident ID and a severity level of Warning, Info, or Debug.

Each Policy server has a distinct and separate set of Trace Log notifications for incidents that occurred on that server. Use the CMP to view the Trace Log notifications from a different server in a cluster. Select the appropriate server from the list at the top of the Trace Log Viewer page.

Syslog

The Syslog receives notifications only from Policy actions. Syslog notifications are directed to a remote syslog host, and the log supports five destinations. Syslog info appears on the MPE Logs tab of the MPE Configuration page.

The SMPP Log

The SMPP log is a policy action-generated notification that contains all Short Message Peer-to-Peer Protocol notifications sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server. In SMPP or XML mode, SMPP info appears on the MPE Logs tab of the MPE Configuration page, under the SMS Log Configuration heading. You can configure the severity of messages that are written to the SMPP log as well as set a forwarding address. For more information, see *Configuring Log Settings*.

The SMTP Log

The SMTP log contains all Simple Mail Transfer Protocol messages sent by the MPE device, as well as any ACK messages received from a mail transfer agent (MTA). In SMPP or XML mode, SMTP Log info appears on the MPE Logs tab of the MPE Configuration page, under the SMTP Log Configuration heading. You can configure the severity of messages that are written to the SMTP log. For more information, see *Configuring Log Settings*.

Configuring Log Settings

From the Logs tab you can configure the log settings for the servers in a cluster. To configure log settings:

1. From the Logs tab, click **Modify**.
   The Modify Settings fields open in the work area.
2. In the **Modify Trace Log Settings** section of the page, configure the Trace Log Level.
   This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164. Adjusting this setting

allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:

- **Emergency** — Provides the least amount of logging, recording only notification of events causing the system to be unusable.
- **Alert** — Action must be taken immediately in order to prevent an unusable system.
- **Critical** — Events causing service impact to operations.
- **Error** — Designates error events which may or may not be fatal to the application.
- **Warning** (the default) — Designates potentially harmful situations.
- **Notice** — Provides messages that may be of significant interest that occur during normal operation.
- **Info** — Designates informational messages highlighting overall progress of the application.
- **Debug** — Designates information events of lower importance.

CAUTION: Before changing the default logging level, consider the implications. Lowering the trace log level setting from its default value (for example, from "Warning" to "Info") causes more notifications to be recorded in the trace log and can adversely affect performance. On the other hand, raising the log level setting (for example, from "Warning" to "Alert") causes fewer notifications to be recorded in the trace log, and could cause you to miss important notifications.

3. In the **Modify Policy Syslog Forwarding Settings** section of the page, configure the syslog forwarding settings. You can direct notifications to up to five remote systems. For each system, enter the following:
   a) **Hostname/IP Addresses** — Remote system hostname or IP address.

CAUTION: Forwarding addresses are not checked for loops. If you forward events on System A to System B, and then forward events on System B back to System A, a message flood can result, causing dropped packets.

   b) **Facility** — Select from Local0 (the default) to Local7.
   c) **Severity** — Filters the severity of notifications that are written to syslog:

      - **Emergency**— Provides the least amount of logging, recording only notification of events causing the system to be unusable.
      - **Alert** — Action must be taken immediately in order to prevent an unusable system.
      - **Critical** — Events causing service impact to operations.
      - **Error** — Designates error events which may or may not be fatal to the application.
      - **Warning** (the default) — Designates potentially harmful situations.
      - **Notice** — Provides messages that may be of significant interest that occur during normal operation.
      - **Info** — Designates informational messages highlighting overall progress of the application.
      - **Debug** — Designates information events of lower importance.

4. In the **Modify SMS Log Settings** section of the page (which only appears when in SMPP mode), configure the following:
   a) **SMPP Log Level** — Indicates the severity of messages that are written to the file SMPP.log.

      Adjusting this setting allows any new events, at or above the configured severity, to be written to the SMPP log.

Note: You can optionally enable the syslog forwarding address for new logs.

Valid levels are:

- **OFF** — Turns off logging.
- **ERROR** — Designates error events which may or may not be fatal.
- **WARN** (the default) — Designates potentially harmful situations.
- **INFO** — Designates informational messages highlighting overall progress.
- **DEBUG** — Designates information events of lower importance.
- **TRACE** — Designates informational events of very low importance.
- **ALL** — Records all logging levels.

b) **SMPP Log Forwarding IP Addresses** — You can forward SMPP.log entries to multiple syslog servers.

5. In the **Modify SMTP Log Settings** section of the page (which only appears when in SMPP mode), configure the **SMTP Log Level**.

   This setting indicates the minimum severity of messages that are recorded in the SMTP log. These severity levels correspond to the syslog message severities from RFC 3164. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the SMTP log. The levels are:

   - **OFF** — Turns off logging.
   - **ERROR** — Designates error events which may or may not be fatal.
   - **WARN** (the default) — Designates potentially harmful situations.
   - **INFO** — Designates informational messages highlighting overall progress.
   - **DEBUG** — Designates information events of lower importance.
   - **TRACE** — Designates informational events of very low importance.
   - **ALL** — Records all logging levels.

6. When you finish, click **OK** (or **Cancel** to discard your changes).
   The log configurations are changed.

Chapter 3

Trace Log Notifications

Topics:

- *Expanded List.....34*

This section lists Trace Log notifications. The incident ID number is also the Trace Log notification ID number. Trace Log notifications may have more than one severity. Each severity is listed with its applicable action.

Expanded List

2 - OSSI collector establishing connection to *type*

Description: The OSSI Collector is trying to connect to a given database address.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

3 - Error occurred during OSSI collector run: *type*

Description: The application that collects information from the OSS has experienced an error.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the OSS database is online and available.

4 - Starting OSSI collector run

Description: The OSSI Collector task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

5 - OSSI collector run completed

Description: The OSSI Collector task has finished its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

6 - OSSI collector run aborted

Description: The application that collects information from the OSS has been cancelled due to user intervention.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

7 - OSSI collector error reading configuration file: *file-name*

Description: Specified configuration file is not present or not readable.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Contact the Tekelec *Customer Care Center*.

8 - OSSI collector established connection

Description: The OSSI Collector task has successfully connected to the OSS database.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

9 - OSSI collector could not establish connection *host port*

Description: The application that collects information from the OSS cannot connect to the OSS network element(s).

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the OSS database is online and available.

12 - OSSI collector did not find configuration parameter: *parameter-name*

Description: The given parameter (e.g., host name, username, or password) for the OSSI Collector task was not configured.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Contact the Tekelec *Customer Care Center*.

13 - Error validating *field*

Description: The OSSI Collector task retrieved a field from the OSS database that's invalid (e.g., a malformed subnet address).

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check the field's value in the OSS database.

14 - Data Collector started

Description: The Data Collector has initialized and started.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

21 - Starting Subnet SNMP Collector task

Description: The Subnet SNMP Collector task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

22 - SNMP timeout while collecting Subnet data from CMTS *name*

Description: The application requesting the subnet data from the network element did not receive a response from the identified network element.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the network element is online and available.

23 - SNMP error *type* while collecting Subnet data from CMTS *name*

Description: The application requesting the subnet data from the network element received an unexpected response.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the network element is online and available.

24 - Skipping Subnet collection from CMTS *name* because the SNMP community string is empty

Description: The Subnet SNMP Collector task cannot poll the given CMTS because the SNMP community string is not configured for it.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

38 - Subnet SNMP Collector Task Status CMTSs

Processed: *n*, Failures: *n*, Subnets Discovered: *n*, Added: *n*, Updated: *n*, Removed: *n*, Elapsed time: *t*sec.

Description: The number of CMTSs processed and the number of subnets discovered by the Subnet SNMP Collector task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

39 - Finishing Subnet SNMP Collector task

Description: The Subnet SNMP Collector task finished its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

41 - Starting Service Class SNMP Collector task

Description: The Service Class SNMP Collector task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

42 - SNMP timeout while collecting Service Class data from CMTS *name*

Description: The application requesting the service class data from the network element did not receive a response from the identified network element.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the network element is online and available.

43 - SNMP error *type* while collecting Service Class data from CMTS *name*

Description: The application requesting the service class data from the network element received an unexpected response.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the network element is online and available.

44 - Skipping Service Class collection from CMTS name because the SNMP community string is empty

Description: The Service Class SNMP Collector task cannot poll the given CMTS because the SNMP community string is not configured for it.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

58 - Service Class SNMP Collector Task Status

CMTSs Processed: *n*, Failures: *n*; Service Classes Discovered: *n*, Added: *n*, Updated: *n*, Removed: *n*, Elapsed time: *t* sec

Description: The number of CMTSs processed and the number of service classes discovered by the Service Class SNMP Collector task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

59 - Finishing Service Class SNMP Collector task

Description: The Service Class SNMP Collector task finished its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

61 - Starting Subscriber SNMP Collector task

Description: The Subscriber SNMP Collector task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

62 - SNMP timeout while collecting Subscriber data from CMTS *name*

Description: The application requesting the subscriber data from the network element did not receive a response from the identified network element.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the network element is online and available.

63 - SNMP error *type* while collecting Subscriber data from CMTS *name*

Description: The application requesting the subscriber data from the network element received an unexpected response.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the network element is online and available.

64 - Invalid cable modem MAC addraess *MAC-address* retrieved from CMTS *name*

Description: The Subscriber SNMP Collector task retrieved an invalid cable modem MAC address from the CMTS.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check the field's value in the network element.

65 - Invalid cable modem IP address *ip-address* for MAC *MAC-address* retrieved from CMTS *name*

Description: The Subscriber SNMP Collector task retrieved an invalid cable modem IP address from the CMTS.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check the field's value in the network element.

66 - Invalid CPE IP address *ip-address* behind cable modem *MAC-address* retrieved from CMTS *name*

Description: The Subscriber SNMP Collector task retrieved an invalid CPE IP address from the CMTS.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check the field's value in the network element.

68 - Skipping Subscriber collection from CMS *name* because the SNMP community string is empty

Description: The Subscriber SNMP Collector task cannot poll the given CMTS because the SNMP community string is not configured for it.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

78 - Subscriber SNMP Collector Task Status

CMTSs Processed: *n*, Failures: *n*; Accounts Discovered: *n*, Added: *n*, Updated: *n*, Removed: *n*, Elapsed time: *t* sec.

Description: The number of CMTSs processed and the number of accounts discovered by the Subscriber SNMP Collector task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

79 - Finishing Subscriber SNMP Collector task

Description: The Subscriber SNMP Collector task finished its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

81 - Starting CMTS Distributor task

Description: The CMTS Distributor task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

82 - Error while sending CMTS data to Policy Server: *name*

Description: The CMP cannot connect to the policy server to push the network element data.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

98 - CMTS Distributor Task Status Policy Server

CMTS processed: *n*, Added: *n*, Updated: *n*, Removed: *n*, Elapsed time: *t* sec.

Description: The number of CMTSs processed by the CMTS Distributor task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

99 - Finishing CMTS Distributor task

Description: The CMTS Distributor task finished its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

101 - Starting Subscriber Distributor task

Description: The Subscriber Distributor task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

102 - Error while deleting Subscriber data from Policy Server: *name*

Description: The CMP cannot connect to the policy server to modify the subscriber data.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

103 - Error while updating CMTS data on Policy Server: *name*

Description: The CMP cannot connect to the policy server to modify the network element data.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

104 - Error while sending *Reconfigure* message to Policy Server: *name*

Description: The CMP cannot communicate a new configuration for the policy server.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

105 - Error while sending *Refresh Channels* message to Policy Server: *name*

Description: Communication problem between CMP/management agent and the policy server during a data refresh of a channel info change request.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

106 - Error while sending *Refresh Accounts* message to Policy Server: *name*

Description: Request for change to account information failed sending to policy server from the CMP.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

107 - Error while sending Tier data to Policy Server: *name*

Description: The subscriber/account tier information configured in the CMP did not push successfully to the policy server.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

108 - Error while sending Channel data to Policy Server: *name*

Description: The channel information for the respective network element was not communicated to the appropriate policy server from the CMP.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the policy server is online and available.

118 - Subscriber Distributor Task Status

CMTSs: *n*, Accounts processed: *n*, Added: *n*, Updated: *n*, Removed: *n*, Elapsed time: *t* sec.

Description: The number of CMTSs and accounts processed by the Subscriber Distributor task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

119 - Finishing Subscriber Distributor task

Description: The Subscriber Distributor task finished its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

121 - Starting OSSI Distributor task

Description: The OSSI Distributor task is starting its scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

122 - Error occurred during OSSI distributor run: *type*

Description: Failed to send data to the Management Agents.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Contact the Tekelec *Customer Care Center*

123 - OSSI distributor run aborted

Description: A user cancelled the distribution of the OSS information within the CMP to the appropriate Management Agents.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

124 - Error connection to Remote MA: *host-name*

Description: The CMP could not establish a connection to the Management Agent.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the Management Agent is online and available.

125 - Error updating Accounts to remote MA:*host-name*

Description: The CMP cannot connect to the Management Agent in order to update account information..

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the Management Agent is online and available.

126 - Error updating CMTSs to remote MA: *host-name*

Description: The CMP cannot connect to the Management Agent in order to update the network element information.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the Management Agent is online and available.

127 - Error updating Tiers to remote MA: *host-name*

Description: The CMP cannot connect to the Management Agent in order to update the subscriber tier information.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the Management Agent is online and available.

128 - Error updating Entitlements to remote MA: *host-name*

Description: The CMP cannot connect to the Management Agent in order to update subscriber entitlement information.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the Management Agent is online and available.

139 - Finishing OSSI Distributor task

Description: The OSSI Distributor task is completing a scheduled run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

141 - Starting CMTS MA Collector task

Description: The CMTS MA Collector task is starting its run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

142 - Error while collecting CMTS data from Management Agent: *name*

Description: The CMP cannot collect the assigned network element information from the Management Agent.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check that the Management Agent is online and available.

157 - CMTS MA Collector task status

MA, CMTS processed: *n*, Updated: *n*, Skipped: *n*, Elapsed time: *t* sec.

Description: The CMP displays the CMTS MA Collector task status.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

158 - CMTS MA Collector Task Status

MAs processed: *n*, CMTS processed: *n*, Updated: *n*, Skipped: *n*, Elapsed time: *t* sec.

Description: The CMTS MA Collector task results are displayed.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

159 - Finishing CMTS MA Collector Task

Description: Th CMTS MA Collector task is ending.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

161 - Starting Pcmm Routing Distribution task

Description: The PCMM routing distribution task is starting.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

177 - PCMM Distribution Task Status

MPE: *n*, Status: *status-number*, Elapsed time: *t* sec.

Description: The PCMM distribution task displays the status of the MPE.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

178 - PCMM Distribution Task Status

MPEs processed: *n*, Updated: *n*, Failed: *n*, Elapsed time: *t* sec.

Description: The CMP displays the status of the PCMM Distribution task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specific cause.

179 - Finishing PCMM Routing Distribution task

Description: The PCMM routing distribution task is ending.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

180 - Task *task - name* was run manually

Description: The operator ran the specified task manually.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

If the message indicates any failures, check the system logs for specified cause.

201 - Start Healthchecker task

Description: HealthChecker task is starting its run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

219 - Finishing Healthchecker task

Description: Healthchecker task is completing its run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

220 - Starting AlertAging task

Description: The AlertAging task is starting its run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

239 - Finishing AlertAging task

Description: The AlertAging task is ending its run.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

241 - OM Statistics collection complete and data is available for request

Description: Data has been saved and is available for OSSI requests, prior to final cleanup tasks.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

276 - Statistics Rsync Cleanup task completed successfully

Description: Statistics Rsync Cleanup task completed successfully.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

278 - Statistics Rsync Cleanup Task failed

error-msg

Description: Statistics Rsync Cleanup Task failed.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Contact the Tekelec *Customer Care Center*.

279 - Finished Statistics Rsync Cleanup Task

Description: Finished Statistics Rsync Cleanup Task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

401 - Starting Stats Files Generator Task

Description: Starting Stats Files Generator Task in the DC process, which generates stats files from OSSI query.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

402 - Stats Files Generator Task completed successfully

Description: Stats Files Generator Task was completed successfully in the DC process.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

403 - Stats Files Generator Task failed #1, 2, 3, or 4

Description: Error log indicating stats files generator task #1, 2, 3, or 4 failed. A Warning trace log is generated for troubleshooting.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Use content of trace log to troubleshoot error.

404 - Finishing Stats Files Generator Task

Description: Info log generated at the completion of a stats files generator task. To verify these stat files, navigate to the local repository defined in this task configuration.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

406 - Sync utility failed to sync stats files to mates. Reason: *reason*

Description: Error log generated when the sync utility failed to sync stats files to mates. The reason for failure is listed in log message.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

1. Based on the failure message, check the server exchange SSH Key in CMP site1 Cluster and site2 Cluster.
2. Check the network connection status to other servers in both Clusters.

407 - Stats Files Generator Task has removed some files which were not synced to remote servers (…)

Description: Warning log generated when a stats files generator task has removed some files which were not synced to remote servers, which includes remote server IP address. Stats files are kept for the period of time defined in the task setting. If these stats files have always been synced to the remote server, this task raises a Warning trace log.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check status of starting stats files synchronization #1,2,3,and 4, and ensure the Enabled stats were configured normally and successfully.

501 - Starting Stats Files Synchronization # 1, 2, 3, or 4

Description: Info log generated when task 1, 2, 3, or 4 of the stats files synchronization to remote servers begins. The task name suffix number indicates different synchronization tasks.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

502 - Stats Files Synchronization #1, 2, 3, or 4 completed successfully.

Description: Info log generated upon the successful completion of the stats files synchronization for task #1, 2, 3, or 4. The task name suffix number indicates different synchronization tasks.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

503 - Stats Files Synchronization # 1, 2, 3, or 4: Task Failure(s) - failure messages.

Description: Error log generated when stats files synchronization task #1, 2, 3, or 4 fails; cause of failure is listed in log title. The task name suffix number indicates the synchronization task during which the failure occurred.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Use content of trace log to troubleshoot error.

504 - Finishing Stats Files Synchronization # 1, 2, 3, or 4

Description: Info log generated when the stats files synchronization process #1, 2, 3, or 4 has finished.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

No action required.

505 - The Local Repository does not exist, you need to check whether Stats Files Generator Task was executed successfully or not

Description: Error log generated when the local repository does not exist; check whether stats files generator task was executed successfully or not.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Determine whether or not the stats files generator task was executed.

506 - Stats Files Synchronization #1, 2, 3, or 4: Task still failed for sync local repository to remote server (xxx.xxx.xxx.xxx) after retry 3 times

Description: Error log generated when a stats files synchronization task fails to sync local repository to a remote server after three retries.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

1. Determine if the remote server supports an SSH protocol connection.
2. Check the network connection status of the remote server.

507 - Stats Files Synchronization #1, 2, 3, or 4: Task was successful for sync local repository to remote server (xxx.xxx.xxx.xxx) after retry 2 times

Description: Warning log generated when a stats files synchronization task successfully syncs the local repository to a remote server after two retries.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: DC

Group: Data Collection Task

Recovery:

Check the network connection status of the remote server.

1004 - PCMM: Lost connection with AM *id*

Description: The MPE device lost a connection from the specified application manager (AM) or upstream policy server (PCMM Router).

Note: Because of protocol limitations, the MPE device cannot distinguish between an AM and a PCMM router, so it always identifies the incoming connection as an AM.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: PCMM

Recovery:

1. Check availability of the AM.
2. Check the AM log for a recent failover or other operation(s) that can interrupt communications.
3. If the AM has not failed, make sure the path from the AM to the MPE device (port 3918) is operational.

1010 - PCMM: Received *msg-type* from AM *id*

msg-contents

Description: The specified message type was received from the specified AM (or upstream policy server).

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

No action required.

1011 - PCMM: Sending *msg-type* to *id*

msg-contents

Description: The specified message type was sent to the specified CMTS (or downstream policy server).

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

No action required.

1012 - PCMM: Received *msg-type* from *id*

msg-contents

Description: The specified message type was received from the specified CMTS (or downstream policy server).

Note: This message is logged at the Warning level when the PCMM message is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

Severity: Info, Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

Contact the Tekelec *Customer Care Center*.

1013 - PCMM: Sending *msg-type* to AM *id*

Description: The specified message type was sent to the specified AM (or upstream policy server).

Note: This message is logged at the Warning level when the PCMM message is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

Severity: Info, Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

Contact the Tekelec *Customer Care Center*.

1014 - PCMM: Failed (*num* attempts) to send *msg-type* event message to *id*

msg-contents

Description: A PCMM event message could not be transmitted to the specified record keeping server (RKS).

Note: The last attempt that fails is logged as an error. If there are additional retries to be attempted then this is logged as a Warning.

Severity: Warn, Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. Check the configuration and availability of the RKS.
2. Ensure the network path from the MPE device to the RKS is available.

1015 - PCMM: Successfully sent *msg-type* event message to *id*

msg-contents

Description: A PCMM event message was successfully sent to the specified RKS.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

No action required.

1016 - PCMM: Failover initiated for RKS *id*, reverting to *id*

Description: The system has lost communication with the primary RKS, and is attempting to establish a connection with the secondary RKS. The identities of both the primary and secondary RKSs are specified.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. Check the configuration and availability of the RKS.
2. Ensure the network path from the MPE device to the RKS is operational.

1017 - Failed (TOO BUSY) to send *msg-type* event message to *id*

msg-contents

Description: The MPE device is unable to send an event message to the specfied RKS because the send queue is too full.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: PCMM

Recovery:

This is normal behavior under heavy PCMM load. It can also occur if there is a communication problem with the RKS because the send queue may fill while the retry messages are being sent.

1020 - PCMM: Rejecting *msg-type* - no PEP available for SubID *IP;* trap will be sent to NM

Description: A PCMM message was received with the specified subscriber IP address but there is no configured CMTS (or downstream policy server) to handle this request.

Note: The request will be rejected with a PCMM error code of 13 (Invalid SubscriberID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. Check the configuration of the CMTSs associated with this MPE device. Make sure that there is a CMTS configured with a subnet for the specified subscriber AND make sure that this CMTS is associated with this MPE device.

2. Check the configuration of the AM sending the message to make sure it is sending the request to the correct MPE device.

1021 - PCMM: Rejecting *msg-type* - invalid gate ID *gateid*

Description: A PCMM message was received with a GateID that does not correspond to any sessions in the MPE database. This checking is only performed if the CMP has enabled Gate checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 2 (Unknown GateID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the flow of messages between the AM, the MPE device, and the CMTS to determine if there are errors in the message forwarding.

1022 - PCMM: Rejecting *msg-type* - AMID mismatch - request *msg-amid* doesn't match gate MPE-AMID

Description: A PCMM message was received with an AMID that does not match the AMID for the corresponding session in the MPE database. This checking is only performed if the CMP has enabled Gate checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 14 (Unauthorized AMID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the flow of messages between the AM and the MPE device to determine if there are errors in the message processing.

1023 - PCMM: Rejecting *msg-type* - SubId mismatch - request *msg-id* doesn't match gate *mpe-id*

Description: A PCMM message was received with a Subscriber ID that does not correspond to a provisioned subscriber in the MPE database of known subscribers (CPEs). This checking is only performed if the CMP has enabled Gate checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 13 (Invalid SubscriberID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the flow of messages between the AM and the MPE device to determine if there are errors in the message processing.

1024 - PCMM: Rejecting *msg-type* - Unrecognized Subscriber *id*

Description: A PCMM message was received with a Subscriber ID that does not correspond to a provisioned subscriber in the MPE database of known subscribers (CPEs). This checking is only performed if the CMP has enabled Subscriber checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 13 (Invalid SubscriberID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the OSS system you are using to provision subscribers for the MPE device to make sure that this subscriber is provisioned.

1025 - PCMM: Rejecting *msg-type* - Unauthorized AmID *id*

Description: A PCMM message was received with an AMID that does not correspond to any know Application in the MPE device. This checking is only performed if the CMP has enabled AMID checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 14 (Unauthorized AMID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the application definitions in the CMP and make sure that this AMID is associated with the appropriate application.
3. Make sure that the application is also associated with this MPE device in the CMP.

1026 - PCMM: Rejecting *msg-type* - Unrecognized Service Class Name *name*

Description: A PCMM message was received with a Service Class Name that does not correspond to any service class that is known to exist for the CMTS to which this message is being sent. This checking is only performed if the CMP has enabled Gate Data checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 11 (Undefined Service Class).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the set of Service Class names that are provisioned for the CMTS in the CMP and make sure that the specified name is included.
3. Make sure the set of Service Class names in the CMP is consistent with the set of values on the actual CMTS.
4. Make sure that the AM is sending the correct value.

1027 - PCMM: Rejecting *msg-type* - Incompatible Envelopes -*env-type* ENV exceeds *env-type* ENV

Description: A PCMM message was received with incompatible Authorized, Reserved and Committed envelopes (QOS parameter specifications). This checking is only performed in the CMP has enabled Gate Data checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 12 (Incompatible Envelope).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the configuration of the AM because this is an indication that it is requesting parameters that violate the protocol specification.

1028 - PCMM: Rejecting *msg-type* - Classifier count exceeds CMTS limit

Description: A PCMM message was received with more classifiers than the provisioned limit for the CMTS to which this message is being sent. This checking is performed only if the CMP has enabled Gate Data checking for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 15 (Number of Classifiers not Supported).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: PCMM

Recovery:

1. If you do not want this checking to be performed, disable it in the CMP.
2. Check the Classifier Limit that is provisioned for the CMTS in the CMP and make sure that it is consistent with the actual CMTS.
3. Make sure your AM is configured to make requests that do not exceed the CMTS limit.

1029 - PCMM: Rejecting *msg-type* - I/O Error while sending to *id*

Description: There was no PCMM session connection to the target CMTS (or downstream policy server).

Note: The request will be rejected with a PCMM error code of 255, and a subcode of 211.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: Diameter

Recovery:

Check the network connectivity between systems.

1101 - DQOS: Established connection to *id*

Description: A new connection was established to the specified CMTS or downstream policy server.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: DQOS

Recovery:

Contact the Tekelec *Customer Care Center*.

1102 - DQOS: Lost connection to *id*

Description: The connection was lost to the specified CMTS or downstream policy server.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: DQOS

Recovery:

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, make sure the network path from the MPE device to the element (port 3918) is operational.

1104 - DQOS: Lost connection with CMS *id*

Description: The MPE device lost a connection from the specified CMS.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: DQOS

Recovery:

Check availability of the CMS.

1110 - DQOS: Received *msg-type* from CMS *id*

Description: The specified message type was received from the specified CMS.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: DQOS

Recovery:

No action required.

1111 - DQOS: Sending *msg-type* to *id*

Description: The specified message type was sent to the specified CMTS.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: DQOS

Recovery:

No action required.

1112 - DQOS: Received *msg-type* from *id msg-contents*

Description: The specified message type was received from the specified CMTS.

Severity: Info, Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: DQOS

Recovery:

This message is logged at the Warning level when the DQOS message is an error message such as GAteSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

1113 - DQOS: Sending *msg-type* to CMS *id*

Description: The specified message type was sent to the specified CMS.

Severity: Info, Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: DQOS

Recovery:

This message is logged at the Warning level when the DQOS message is an error message such as GAteSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

1120 - DQOS: Rejecting *msg-type* - no CMTS available for SubID *id*

Description: A DQOS message was received with the specified subscriber IP address but there is no configured CMTS to handle this request.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: DQOS

Recovery:

Check the configuration of the CMTSs associated with this MPE device. Make sure that there is a CMTS configured with a subnet for the specified subscriber AND make sure that this CMTS is associated with this MPE device.

1121 - DQOS: Rejecting *msg-type* - invalid gate id *id*

Description: A DQOS message was received with a GateID that does not correspond to any session in the MPE database. This checking is only performed if the CMP has enabled Gate checking for the MPE device (by default this is off).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: DQOS

Recovery:

If you do not want this checking to be performed, disable it in the CMP.

1123 - DQOS: Rejecting *msg-type* - SubId mismatch - request *msg-id* doesn't match gate *mpe-id*

Description: A DQOS message was received with a Subscriber ID that does not match the Subscriber ID for the corresponding session in the MPE database. This checking is only performed if the CMP has enabled Gate checking for the MPE device (by default this is off).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: DQOS

Recovery:

If you do not want this checking to be performed, disable it in the CMP.

1124 - DQOS: Rejecting *msg-type* - Unrecognized Subscriber *id*

Description: A DQOS message was received with a Subscriber ID that does not correspond to a provisioned subscriber in the MPE database of known subscribers (CPEs). This checking is only performed if the CMP has enabled Subscriber checking for the MPE device (by default this is off).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: DQOS

Recovery:

If you do not want this checking to be performed, disable it in the CMP.

1129 - DQOS: Rejecting *msg-type* - DQOS I/O Error while sending to *id*

Description: An unexpected I/O error was encountered while trying to send the specified message to a CMTS.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: DQOS

Recovery:

1. Check the logs for further details on the I/O error.
2. Check the availability of the destination CMTS and the operational status of the network to the CMTS.

1150 - DQOS: Rejecting msg-type - Rejected by policy name

Description: There was no PCMM session connection to the target CMTS (or downstream policy server).

Note: The request will be rejected with a PCMM error code of 255, and a subcode of 211.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: DQOS

Recovery:

Check the network connectivity between systems.

1204 - SPC DQOS: Lost connection with CMS *id*

Description: The MPE device lost a connection from the specified CMS.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

1. Check availability of the CMS.
2. Check the CMS log for a recent failover or other operation(s) that can interrupt communications.
3. If the CMS has not failed, make sure the path from the CMS to the MPE device (port 2126) is operational.

1209 - SPC DQOS: Deleting gate *gateid*, T1 Timer expired

Description: The specified gate was deleted because it did not transition from the RESERVED state to the COMMITTED state before the T1 Timer expired.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

Check the logs and status in the CMS to determine why the gate did not get committed. This may be a normal situation in which the call was aborted before it was fully set up.

1210 - SPC DQOS: Received *msg-type* from CMS *id msg-contents*

Description: The specified message type was received from the specified CMS.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

Contact the Tekelec *Customer Care Center*.

1213 - SPC DQOS: Sending *msg-type* to CMS*id*

Description: The specified message type was sent to the specified CMTS. If the message is reporting an error, then this message is logged at the Warning level, otherwise it is logged at the Info level.

Severity: Info, Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

Contact the Tekelec *Customer Care Center*.

1221 - SPC DQOS: Rejecting *msg-type* - invalid global session id *globalsessionid*

Description: The MPE device received a request to perform an operation on a global session (call) that does not exist in the MPE database.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

1. This is usually an indication that there is a protocol error or communication problem between an MPE device and a CMS.
2. If there was a recent failover or communication interruption it is possible that one of the devices may have data that is not complete.

1231 - SPC DQOS: Rejecting *msg-type* - invalid ingress id *ingressid*

Description: The MPE device received a request to set up a gate for a zone that does not exist (as specified by the ingress ID in the request).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

Ensure that the topology information in the MPE device is up-to-date and consistent with the topology information in the CMS that issued the request.

1232 - SPC DQOS: Rejecting *msg-type* - no path to root zone for ingress id *ingressid*

Description: The MPE device received a request to set up a gate for a zone that does not have a valid path to the root zone.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

Although in theory this is possible, it should not happen unless there is a problem in the configuration of the network topology. Verify that the network topology is defined correctly.

1233 - SPC DQOS: Dropping *msg-type* - invalid gate id *gateid*

Description: The MPE device received a request that referenced the specified gate ID and an unrelated session (via the GlobalSessionID).

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: SPC DQOS

Recovery:

1. This is usually an indication that there is a protocol error or communication problem between an MPE device and a CMS.
2. If there was a recent failover or communication interruption, it is possible that one of the devices may have data that is not complete.

1314 - NAC: Abnormal delete of session

session-detail, Reason Code: *code*, Text: *reason text*

Description: Session deleted abnormally. An element-level stat in the MPE tracks total normal disconnects per network element. The CMP retrieves this stat as part of the current call for network element stats using the OM Stats Task.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: NAC

Recovery:

Contact the Tekelec *Customer Care Center*.

1315 - NAC: Normal delete of session

session-detail

Description: The session is deleted normally. *session-detail* includes the Subscriber ID, the format of which changes depending on whether the subscriber has a dynamic or static IP address (static IP subscribers do not have the @BRAS on their ID). An element-level stat in the MPE tracks total normal disconnects per network element. The CMP retrieves this stat as part of the current call for network element stats using the OM Stats Task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: NAC

Recovery:

No action required.

1316 - NAC: Allowed session

session-detail

Description: The MPE allowed the session. Upon completion of each session request (blocked or allowed) from the VoD server, the MPE generates an Info level event log. The following data is provided within the message: reason code (if applicable), account id, subscriber data, network element name, full network path.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: NAC

Recovery:

No action required.

1320 - NAC: Rejecting *msg-type* - no path available from *SUB-IP* to *SERVER-IP*

Description: A request was received but there was no provisioned path that could be used to satisfy the endpoints in the request.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: NAC

Recovery:

1. Check the specified SUB-IP and Server-IP and determine if there is a path that should be used.
2. If such a path exists, make sure that the B-RAS in the path is actually associated with the MPE in the CMP.

1321 - NAC: Rejecting *msg-type* - subscriber with address *SUB-IP* is unknown (session ID *VoD-ID*)

Description: A subscriber without an associated account requested a VoD session. The session request was denied.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: NAC

Recovery:

1. Check to make sure that there is an account for the specified subscriber in the OSS.
2. Make sure that the name fo the network element in the account is a B-RAS that is associated with the MPE in the CMP.

1322 - NAC: Allowing *msg-type* - subscriber with unknown address *SUB-IP* (session ID *VoD-ID*)

Description: A subscriber without an associated accouant requested a VoD session. The session request was allowed.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: NAC

Recovery:

Contact the Tekelec *Customer Care Center*.

1323 - NAC: No account information for subscriber *SUB-IP* (session ID *VoD-ID*)

Description: A subscriber with dynamic IP address *SUB-IP* without an associated account requested a VoD session. The session request was denied.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: NAC

Recovery:

Contact the Tekelec *Customer Care Center*.

1324 - NAC: Subscriber with address *SUB-IP* is unknown (session ID *VoD-ID*)

Description: A subscriber with an unknown IP address requested a VoD session. The subscriber does not have a static IP address assigned to it, and the subscriber's associated BRAS has not notified the MPE that it has attached to the network. If event 1324 is generated, either event 1321 or 1322 is also generated.

Severity: Warn

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: NAC

Recovery:

Contact the Tekelec *Customer Care Center*.

1351 - NAC: Both static and dynamic definitions for subscriber IP address *SUB-IP*, using dynamic definition

Description: In making a video request, a subscriber added a static IP address to an account, but the BRAS to which the subscriber is connected also assigned it a dynamic IP address.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: NAC

Recovery:

Either remove the static IP definition or configure the subscriber on the BRAS to have a static IP address.

1352 - NAC: Could not find BRAS endpoint *endpoint* in path *path* - rejecting

Description: An IP subnet pool is improperly associated with a newtwork element (For example, subnet 10.1.x.x is associated with NE1, but NE2 has assigned a subscriber in the same range.)

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: NAC

Recovery:

Ensure that the IP subnet ranges do not overlap on the network elements.

1370 - BRAS: COPS-PR declared an IP address (*ip*) already defined as static in account *account*

Description: A subscriber attached to the network with a static IP address but the BRAS to which the subscriber is connected also assigned a dynamic IP address.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: BRAS

Recovery:

Either remove the static IP definition or configure the subscriber on the BRAS to have a static IP address.

1401 - Diameter: Transport connection opened with peer *peer_id*

Description: A transport level connection (such as TCP) has been established with a Diameter peer.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

No action required.

1402 - Diameter: Transport connection closed with the peer *0*

Description: Connection to the network element or HSS is closed by peer *0*, where *0* is the IP address of the peer + port.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Diameter

Recovery:

Verify that the peer is online (although the connection can recover on its own on the next retry attempt).

1403 - Diameter: Transport connection disconnected by the peer *0*

Description: Connection to network element or HSS is disconnected by peer *0*, where *0* is the IP address of the peer + port.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Diameter

Recovery:

Verify that the peer is online (although the connection can recover on its own on the next retry attempt).

1404 - Diameter: Sent msg to peer *peer_id* connection *conn_ id*

Description: A Diameter message has been sent to a peer.

Severity:

- Warning - when message contains an error
- Info - for Debug normal messages
- Debug - for Diameter Watchdog requests and answers

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

No action required.

1405 - Diameter: Received msg from peer *peer_id* connection *conn_id*

Description: A Diameter message has been sent to a peer.

Severity:

- Warning - when message contains an error
- Info - for Debug normal messages
- Debug - for Diameter Watchdog requests and answers

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

No action required.

1406 - Diameter: Error processing message msg from peer *peer_id* connection *conn_id*

Description: An error occurred while processing a received message.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

No action required.

1407 - Diameter: Peer id (*connection_id*) status changed from *previous_status* to *new_status*

Diameter: Peer id (*connection_id*) status changed from *previous_status* to *new_status*

Description: The status of a Diameer peer has changed. This event is usually generated after a connection has been established and capability exchange has occurred.

Severity:

- Info - after a connection has been established and capability exchange has occurred
- Error - after a connection was torn down with a peer

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

No action required.

1408 - Diameter: New connection rejected

Description: A Diameter peer (identified by its Diameter Identity) attempted to establish a connection with the Camiant device although it already has a valid connection. The Diameter protocol allows only one connection from a particular peer.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Diameter

Recovery:

Check connectivity with peer; contact the Tekelec *Customer Care Center*.

1409 - Diameter: Rejecting *msg_type* from *peer_id - con_id* AVP(s) not found in request *request_details*

Description: Request was rejected by the Policy Management device as it was missing an AVP that was required for the processing of the request based on the corresponding Diameter application procedures and current session state.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

Check the peer configuration to identify the reason the AVP was not included in the request.

1410 - Diameter: Response timeout for *msg_type* sent to *conn_id msg_details*

Description: A response message was not received for the request sent to the destination host.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

If the problem persists, contact Customer Support.

1411 - Diameter: Received Duplicate message *msg_type* from *conn_id msg_details*

Description: The received message was discarded because it was received previously by another message containing the same Diameter End-to-End Identifier from the same origin host.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

If the problem persists, contact Customer Support.

1412 - Diameter: Sent *{type} to {destination} in {connection ID} mes {message}*

Description: A Diameter message was sent.

Severity:

- Info - for Debug normal messages
- Debug - for Diameter Watchdog requests and answers

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

If the problem persists, contact Customer Support.

1413 - Diameter: Received *{type} from {sender} in {connection ID} mes {message}*

Description: A Diameter message was received.

Severity:

- Info - for Debug normal messages
- Debug - for Diameter Watchdog requests and answers

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

If the problem persists, contact Customer Support.

1414 - Diameter: SCTP path on association ID address ADDR_CONFIRMED/ADDR_UNREACHABLE/ADDR_AVAILABLE

Description: An SCTP path is unavailable. An info level message is generated when a backup or non-primary path is confirmed by the SCTP association. An error level message is generated when one of the paths fails, whether it is a primary or non-primary path. A notice level message is generated when a path that previously failed recovers.

Severity: Info, Notice, Warning

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

If the problem persists, contact Customer Support.

1420 - Diameter: Rejecting *application_request* - no PCEF available for subscriber

Description: Request from an application function (such as P-CSCF) was rejected by the MPE device as there was no corresponding session with the PCEF (such as a GGSN) for the subscriber.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

Check the provided subscriber identification and IP address and verify that it corresponds to a subscriber who is attached to the network.

1421 - Diameter: No default QoS profile defined for media *type*

Description: The MPE device received a request (such as Rx) from an application to set up policy rules on the enforcement device, but the application function did not provide enough information in the request for the device to derive corresponding quality of service parameters, and there are no default profiles configured in the device for the corresponding media type.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

Check the MPE device configuration for Diameter AF default QoS profiles and add a default QoS profile for the media type in question. Verify the reason why the application function did not provide enough info to the device within the application request.

1440 - Diameter: Rejecting request for subscriber *sub_id* - No Network Element found for node *node_id*

Description: The MPE device rejected a request (such as Gx) from an enforcement device (such as a GGSN) because it did not recognize it as a "known" network element.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

Check the MPE device configuration and verify that the enforcement device is configured as a Network Element and associated with the MPE device. Also, verify that the Network Element's Diameter identity is configured.

1441 - Diameter: PCC rule *rule* failed for subscriber *sub_id xxx* - Rule failure code *code*

Description: A PCEF Charging-Rule-Report indicated that installation of the specified PCC rule for the specified subscriber and Diameter session failed with the specified failure code. If the PCEF reports failure to install multiple rules for the same reason, the MPE device generates a single event with multiple rule names.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

No actions are required.

1442 - Diameter: PCC rule *rule* retry *x* of *y* for subscriber *sub_id xxx*. Next retry in *z* seconds.

Description: The MPE device retry installation of the specified PCC rule for the specified subscriber and Diameter session in the specified number of seconds.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

No actions are required.

1443 - Diameter: PCC rule *rule* retry failed after *n* attempts for subscriber *sub_id xxx*

Description: Installation of the specified PCC rule failed the maximum configured number of times for the specified subscriber and Diameter session.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

Check network connectivity, and if necessary adjust configuration values.

1444 - Diameter: PCC rule *rule* retry canceled for subscriber *sub_id xxx*

Description: Retrying installation of the specified PCC rule was canceled for the specified subscriber and Diameter session. This can happen because the rule was removed as the result of a policy action.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

No actions are required.

1445 - Diameter: PCC rule *rule* retry aborted for subscriber *sub_id xxx* - Too many retries in progress (*n* attempts)

Description: A rule installation retry cannot be initiated because the maximum number of simultaneous retries has been reached.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

If necessary, adjust configuration values.

1446 - Diameter: The maximum number of PDN connections has been exceeded for subscriber *ID*

Description: The maximum number of PDN connections has been exceeded for a subscriber.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Diameter

Recovery:

No actions are required

1450 - SceGX: No SCE Profile or Default Profile set for subscriber *subscriber*

Description: For the given subscriber, there was no SCE Package ID set either via an SCE Traffic Profile in policy or via the Diameter PCEF Default Profile.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

Ensure all subscribers have an SCE Traffic Profile applied to their CCRi request, either via policy or by selecting an SCE Traffic Profile as the Diameter PCEF Default Profile.

1470 - Begin diameter session binding cleanup task

Description: The diameter session binding cleanup task has begun.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

No action required.

1471 - End of database iterations

Description: The database iterations (listing the potential number of stale sessions identified for cleanup) have ended.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

No action required.

1472 - End of diameter session binding cleanup task

Description: The purging process has started and the diameter session binding cleanup task has ended.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

No action required.

1600 - DBPLUGIN: No matches for *criteria*, search type *ID*

Description: DbPlugin search request did not find any results

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1601 - LDAP: Established Connection to *srv*

Description: A new connection to the indicated server was established.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required.

1602 - LDAP: Closing conection to *srv*

Description: The connection to the indicated server was closed.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required.

1605 - LDAP: Attempted connection to *0* failed, reason: *1*

Description: The connection to the indicated server failed for the reason specified.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

Check LDAP data source configuration to verify proper connection information is provided.

1610 - LDAP: Search failure for *ID* due to the following error: *error message*

Description: LDAP search failure due to an error.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1611 - LDAP: Searching for *stype: criteria*

Description: A search is being performed for the search type *stype* using the indicated criteria.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required.

1612 - LDAP: Search results for *stype filter* are *results*

Description: Displays the results of the search request (if matches found).

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required.

1613 - LDAP: No matches for *stype filter*

Description: A search returned no results.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

With multiple data sources, an individual data source might not return any results.

1614 - LDAP: Multiple matches for *stype filter*

Description: A search returned multiple results.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

Verify that the search criteria should have resulted in multiple matches. If necessary, correct the LDAP configuration.

1615 - LDAP: Unexpected search failure for *stype filter*, reason: *msg*

Description: A search was terminated because of an unexpected exception

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

Verify that the search criteria should have resulted in multiple matches. If necessary, correct the LDAP configuration.

1617 - LDAP: Detailed description of LDAP modification to be initiated

Description: This is a detailed description of the LDAP modification to be initiated. Example - Modify Entry for *Processor ID* (for example *UserByE164*); LDAP Processor: *Processor ID* Entry DN: *LDAP DN* Attribute: *LDAP Attribute* Value: *new value*

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No action required.

1619 - LDAP: Unexpected modify failure for *process ID key*, reason: *message*

Description: Unexpected LDAP modify failure.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1620 - LDAP: Operation queue *process ID* in distress. Queue capacity exceeds *event message*.

Description: An LDAP operations queue is in distress and has exceeded capacity.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1621 - LDAP: Operation queue *process ID* has cleared and is no longer in distress. Capacity is below *event message*

Description: An LDAP message queue is no longer in distress

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1622 - LDAP:Operation queue *process ID* is currently at 100% and will begin rejecting new LDAP Modify requests.

Description: An LDAP message queue is at 100% capacity and will reject new LDAP modify requests.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1623 - LDAP:Modify failure. Unable to modify *fields* at *distinguished name* due to the following error: *message*

Description: Unable to initiate an LDAP modify operation on the specific External Field specified by the user. Example - Modify failure. Unable to modify *External Field Name* at *LDAP DN* due to the following error: *reason*

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1624 - LDAP:Modify failure. Unable to perform modify due to the following error: *message*

Description: Unable to initiate an LDAP modify operation because the LDAP data source does not support this operation. Example - Modify failure. Unable to perform modify due to the following error: Data source is not configured with External Fields and will not support this update.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1626 - LDAP:Update unsuccessful: *message*

Description: Successful LDAP update.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1661 - SH:Peer Realm *detailed message*

Description: SH bad realm configured

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1662 - SH:Bad *primary/secondary* address *reason*

Description: SH bad IP address configured

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1663 - SH:Searching for *peer ID*: *query*

Description: Started search for user in Diameter Peer HSS

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1664 - SH:Search results for *query peer ID* are: *error message*

Description: Search results for user from Diameter Peer HSS

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1665 - SH:No matches for *peer ID query*

Description: No results found for user from Diameter Peer HSS

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1666 - SH:Unexpected search failure on *peer ID*

Description: Unexpected SH search failure.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1667 - SH:Subscribing for *sub type name*: *element*

Description: SH: Subscribing for user profile change notifications for a user.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1668 - SH:Subscription results for *user ID type element* are: *response*

Description: Subscription results for user from DIameter Peer HSS.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1669 - SH:Unexpected subscription failure for *user ID type element*, reason: *response*

Description: SH: Unexpected subscription failure.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1670 - SH:Unsubscribing for *sub type name*: *element*

Description: SH: Unsubscribing for user profile change notifications for a user.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1671 - SH:Unsubscription results *user ID type element* are: *response*

Description: SH: Unsubscription results for user from Diameter Peer HSS.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1672 - SH:Unexpected unsubscription failure *user ID type element* are: *response*

Description: SH: Unexpected unsubscription failure.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1673 - SH:Received notification: *results*

Description: SH: Recieved a notification

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: LDAP

Recovery:

No actions are required

1681 - MSR: Established connection to *ip:port*

Description: A new connection to the server at the specified IP address was established.

Severity: Info, Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1682 - MSR: Closing Connection to *ip:port*

Description: The connection to the server at the specified IP address was closed.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1683 - MSR: Connection to the MSR server at the specified IP address was closed unexpectedly

Description: Connection to the MSR server at the specified IP address was closed unexpectedly.

Severity: Info

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: MSR

Recovery:

Check if the peer is online.

1684 - MSR: Closing a secondary MSR connection to revery to a primary connection

Description: Closing a secondary MSR connection to revery to a primary connection. Occurs when flipping back from secondary to primary MRA connection.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: MSR

Recovery:

Self recovery; no action required.

1685 - MSR: Connection attempt to MSR server failed

Description: Connection attempt to the MSR server at the specified IP address failed for the specified reason.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: MSR

Recovery:

MSR connectivity issue; verify that the peer is online.

1686 - MSR: Searching for *type: key*

Description: A search is being performed for the search type *type* using the specified key.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1687 - MSR: Searching for *type: key*

Description: Search result for *type key* is: *result*

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1690 - MSR: Unexpected search failure for *type key*, reason: *msg*

Description: A search was terminated for the specified unexpected reason.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1691 - MSR: Updating *type: key*

Description: An update is being performed for the update type *type* using the specified key.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1692 - MSR: Update result for *type key* are: *result*

Description: The results of the update request.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1693 - MSR: Unexpected update failure for *type key*, reason: *msg*

Description: An update was terminated for the specified unexpected reason

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1694 - MSR: Subscribing for *type: key*

Description: A subscription is being performed for the subscription type *type* using the specified key.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1695 - MSR: Subscription results for *type key* are: *results*

Description: The results of the subscription request.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1696 - MSR: Unexpected subscription fialure for *type key*, reason: *msg*

Description: A subscription was terminated for the specified unexpected reason.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1697 - MSR: Unsubscribing for *type: key*

Description: An unsubscription is being performed for the subscription type *type* using the specified key.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1698 - MSR: Unsubscription results for *type key* are: *result*

Description: The results of the unsubscription request.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

1699 - MSR: Unexpected unsubscription failure for *type key*, reason: *msg*

Description: An unsubscription was terminated for the specified unexpected reason.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1701 - COPS-PR: Connection accepted from gateway IP *ip-address*, port *port*

Description: A new COPS-PR connection was accepted from the specified gateway. *ip-address* refers to the remote ERX's IP address learned from the COPS socket connection, and *port* refers to the port.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: COPs-PR

Recovery:

Contact the Tekelec *Customer Care Center*.

1702 - COPS-PR: Lost connection with gateway *id*

Description: The MPE lost a connection from the gateway. *id* refers to the remote ERX's IP address learned from the COPS socket connection.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: COPs-PR

Recovery:

1. Check availability of the gateway.
2. If the gateway has not failed, make sure the path from the gateway to the MPE is operational.

1703 - COPS-PR: Rejecting OPN message from *id*. Unknown gateway

Description: An unknown gateway is trying to establish a COPS-PR connection to the MPE. *id* refers to the remote ERX's IP address learned from the COPS socket connection, if it's retrieved. Otherwise, "unknown address" is printed.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: COPs-PR

Recovery:

1. Check the configuration of the network elements in the CMP. There should be a B-RAS network element for this gateway and that B-RAS must be associated with this MPE.
2. Make sure that the configuration of the B-RAS network element is consistent with the provisioned information on the gateway. The network element name in the CMP must match the provisioned router name on the gateway.

1711 - COPS-PR: Received *msg-type* from *id*

Description: The specified message type was received from the specified gateway. *id* refers to the remote ERX's IP address learned from the COPS socket connection.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: COPs-PR

Recovery:

No action required.

1712 - COPS-PR: Sending *msg-type* to *id*

Description: The specified message type was sent to the specified gateway. *id* refers the ERX's IP address learned from COPS socket connection.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: COPs-PR

Recovery:

Contact the Tekelec *Customer Care Center*.

1721 - COPS-PR: Dropping *msg-type* from *id* - *reason*

Description: There was a protocol error while processing the specified COPS-PR message from the specified gateway. *Reason* provides a more detailed description of the specific protocol error that occurred.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: No

Server: MPE

Group: COPs-PR

Recovery:

Contact the Tekelec *Customer Care Center*.

1740 - BRAS: Transmit buffer for *n* extended from *x* to *y*

Description: The transmit buffer has extended from *x* to *y*. *n* refers to the remote ERX's IP address learned from the COPS socket connection.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: BRAS

Recovery:

Contact the Tekelec *Customer Care Center*.

1741 - BRAS: Transmit buffer for *id* shrunk from *x* to *y*

Description: The transmit buffer has decreased from *x* to *y*. *id* refers the ERX's IP address learned from COPS socket connection.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: BRAS

Recovery:

Contact the Tekelec *Customer Care Center*.

1750 - Gx-Plus: Received CCR-I, session ID *x* subid *y* from *id*

Description: The PCRF received a credit control request for an initial request (CCR-I) with session ID *x* and sub id *y* from the gateway *id*. *id* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is printed.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1751 - Gx-Plus: Received CCR-T, session ID *x* from *id*

Description: The gateway *n* sends a CCR-T with a session ID to indicate that a subscriber has logged out and its subscriber data should no longer be associated with an IP address. *id* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is printed.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1756 - Gx-Plus: Learnt new endpoint *id*, *x* from gateway *y*

Description: The PCRF has learned a new subscriber endpoint with *id* as the IP address and *x* as the session ID from the gateway *y*. *y* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE diameter Identity is printed.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1763 - Gx-Plus: Start state synchronization with gateway *id*

Description: The gateway *id* starts a state synchronization with the PCRF. *id* refers to the GX-MX's Host Name/IP Address configured in the GUI Network Elements tab, if it's set. Otherwise, it's empty.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1764 - Gx-Plus: State synchronization with gateway *id* has completed

Description: This event signals the completion of state synchronization between the gateway *id* and the PCRF. *id* refers to the Gx-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is printed.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1765 - Gx-Plus: Drop all the bras endpoints and diameter sessions because of cold reboot from gateway *id*

Description: When the PCRF receives a JSER from the GWR indicating a cold boot event, it purges all the sessions that were created by requests from the gateway *id*. *id* refers to the GX-MX's Host Name/IP Address configured in the GUI Network Elements tab, if it's set. Otherwise, it's empty.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1766 - Gx-Plus: Deleting endpoint *n*, *x* due to CCR-T from gateway *id*

Description: This event is generated when an endpoint is deleted from the PCRF database upon successfully processing a CCR-T message from the gateway *id*. *id* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is printed.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1767 - Gx-Plus: Deleting stale entry for IP *n*, *x* from gateway *id*

Description: Once the state sync is complete or upon receiving a discovery request, the PCRF performs a scrub operation, by which it deletes all the subscriber information for the gateway *id*, which was not reported by the gateway in the JSDA messages. This removes stale entries from the PCRF databases. *id* refers to the GX-MX's IP address the from the session logon.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1768 - Gx-Plus: Received warm reboot message from gateway *id*

Description: When the gateway is warm-booted, the gateway *id* sends a JSER to indicate a warm boot event. *id* refers to the GX-MX's Host Name/IP Address configured in the GUI Network Elements tab, if it's set. Otherwise it's empty.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

1769 - Gx-Plus: Received AYT message from gateway *id*

Description: Occurs when the router receives no response from the PCRF. Can be caused by a broken connection, a PCRF failover, or a router cold boot. The appearance of this log implies the connection between the router and the PCRF has been recovered. *id* refers the GX-MX's Host Name / IP Address configured in the GUI Network Elements tab, if it's set. Otherwise, it's empty.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Gx-Plus

Recovery:

Contact the Tekelec *Customer Care Center*.

2300 - TOD: Time period(s) changed from *prev_time_periods* to *new_time_periods*

Description: The current time period has changed. (This may not affect any sessions).

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required.

2301 - TOD: Transition to time period(s) *new_time_periods* started.

Description: A time period transition has started.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required.

2302 - TOD: Transition to time period(s) *new_time_periods* was still in progress when time periods changed. transition aborted.

Description: A time period transition has started occured before a previous transition was completed.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required.

2303 - TOD: Transition to time period(s) *new_time_periods* successfully completed.

Description: A time period transition has finished, and all affected sessions have been updated accordingly.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required.

2304 - TOD: Transition to time period(s) *new_time_periods* failed to complete normally.

Description: A time period transition was not completed due to a communication failure with the policy enforcement device.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required.

2305 - TOD: Transition to time period(s) *new_time_periods* was aborted

Description: An operator has manually aborted a time period transition.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required.

2306 - TOD:Transition to time period(s) *current time periods* was invoked by the operator.

Description: A transition to a time period was invoked by the operator.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2500 - SCE:Connecting to *SCE ID*

Description: Sce reconfigure event.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2501 - SCE:Lost connection to *SCE ID*

Description: Lost connection to the SCE.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2502 - SCE:Received *request type* for subscriber *sub ID* from *SCE ID*

Description: SCE: Recieved message for subscriber.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2503 - SCE:Sent *request type* for subscriber *sub ID* and package *package ID* to *SCE ID*

Description: SCE: Sent message for subscriber.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2504 - SCE:Sent Logout request for subscriber *sub ID* to *SCE ID*

Description: Send logout request for subscriber.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2505 - SCE:Received error *error message* for *operation name* setting package *package* for subscriber *sub ID* from *SCE ID*

Description: Sce update operation has failed

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2506 - SCE:Error *detailed message* when processing *request type* from *subscriber ID*

Description: Sce quota operation has failed.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2507 - SCE:Re-setting package from *previous package ID* to *new package ID* for subscriber *subscribe ID* at *SCE ID*

Description: Sce connection lost.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2549 - SMS:SMSR internal queue is full: *queue name*.

Description: SMSR internal queue is full: *queue name*. Messages will be rejected until space becomes available.

Severity: Warning

Notification: Trace Log

Alarm: Yes - 72549

Trap: No

Server: MPE

Group: SMS

Recovery:

No actions are required.

2550 - SMS:SMS Relay is not enabled to receive message. *optional additional details*

Description: SMS Relay is not enabled. Info level if occurs during reconfiguration, Warning level occurs if occurs during operation.

Severity: Info, Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2551 - SMS:Configured SMS Relay endpoint: *SMS end point*

Description: Configured SMS Relay endpoint.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2552 - SMS:Sent to id: *ID* using SMS Relay defined at *end point*\n Message:*message*

Description: Send message using SMS Relay.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2553 - SMS:Unable to send SMS to *ID*. Invalid Billing Day *billing day* configured.

Description: Unable to send SMS due to Invalid Billing Day.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2555 - SMS:Error sending SMS to *ID* using SMS Relay defined at *end point*\n Message:*message*

Description: Error sending SMS using defined SMS Relay.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2556 - SMS:Unable to send SMS to *response message* using SMS Relay defined at *end point ID*

Description: Unable to send SMS using defined SMS Relay.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2557 - SMS:Unable to send SMS to *user ID*. User's MSISDN could not be found.

Description: Unable to send SMS due to User's MSISDN not found.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Time-of-Day

Recovery:

No actions are required

2565 - SMTP:Connection has been closed to MTA *IP Address*

Description: Connection is lost to the MTA.

Severity: Warning

Notification: Trace Log

Alarm: Yes - 72565

Trap: No

Server: MPE

Group: SMTP

Recovery:

No actions are required.

2566 - SMTP:Connection established to MTA *IP Address*

Description: SMTP:Connection established to MTA *IP Address*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SMTP

Recovery:

No actions are required.

2567 - SMTP:Error attempting to establish a new connection to *mta*\n Error:*error*

Description: SMTP:Could not establish connection to *MTA IP address*. Reported error message is *error*.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SMTP

Recovery:

No actions are required.

2611 - MSR: Received notification: *msg*

Description: The specified notification was recieved from the MSR about a subscriber profile change.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: MSR

Recovery:

No actions are required.

2700 - New DRA binding created

Description: A DRA new binding was created and an MPE device was selected for the subscriber's sessions.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2701 - RADIUS:Initializing communications on port *port number*

Description: RADIUS: Initializing communications on a specified port.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2701 - DRA binding released between subscriber and MPE device

Description: A DRA binding was released between the named subscriber and MPE device because the subscriber's last session was terminated.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2702 - Existing binding found

Description: An existing binding was found (and possibily updated) between the named subscriber and MPE device.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2703 - RADIUS:Start failed on port *port number*

Description: RADIUS: Failed to start listening on a specified port.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2703 - MRA did not find binding information for subscriber

Description: The MRA did not find binding information for the named subscriber and has to either query another MRA device or respond to a requesting MRA device.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2704 - RADIUS:Received *message code* / status type:*accounting type pocket ID* / *session ID* from *client address.message*

Description: RADIUS: Recieved RADIUS message.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2704 - Binding Release Task *STARTED* | *COMPLETED* | *ABORTED*

Description: The MRA did not find binding information for the named subscriber and has to either query another MRA device or respond to a requesting MRA device.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2705 - RADIUS:Dropping invalid message *request. reason*

Description: RADIUS: Dropping invalid RADIUS message.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2705 - Duplicate bindings have been detected for *list_of_user_ids* on *list_of_MRAs*

Description: The variable *list_of_user_ids* will contain a comma separated list of user ids and *list_of_MRAs* will be a comma separated list of identities of the MRAs that have the duplicate binding.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2706 - RADIUS:Dropping message with bad MD5, probably bad password in *request*

Description: RADIUS: Dropping message with bad MD5COMMA probably bad password.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2706 - Binding cleanup task has been started

Description: Indicates that the cleanup task to look for stale sessions and suspect bindings has started or is currently running.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2707 - RADIUS:Sent *message code* [*accounting status type / pocket ID*] to *session ID.message*

Description: RADIUS: A response to a Radius Accounting message was successfully sent.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2707 - Binding cleanup task is finished and processed *0* stale bindings, *1* duplicate bindings, and *2* stale sessions

Description: Indicates the cleanup task is now finished for its current cycle, and displays the number of stale bindings, duplicate bindings, and stale sessions detected.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MRA

Group: MRA

Recovery:

No actions are required.

2710 - RADIUS:Stopping communication for *port number*

Description: RADIUS: Stopping communication.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: RADIUS

Recovery:

No actions are required

2900 - ADMISSION: System is in busy state because *resource name*: criteria *admission criteria*

Description: The current system load is evaluated by an admission controller as exceeding admission criteria thresholds.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Load Admission

Recovery:

Typically, this condition returns to normal state. If it persists, contact Customer Support.

2901 - ADMISSION: System is in normal state

Description: The current system load is below clearing admission criteria thresholds and stability timeout is exceeded.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Load Admission

Recovery:

No actions are required.

2902 - ADMISSION: Monitored resource *resource-name* is in busy state: criteria *threshold*

Description: The load of the monitored resource is evaluated by an admission controller as exceeding the admission criteria threshold. This event carries only an informative value and can be disabled by the ResourceStateLog property.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Load Admission

Recovery:

Typically, this condition returns to normal state. If it persists, contact Customer Support.

2903 - ADMISSION: Monitored resource *resource-name* is in normal state: criteria *threshold*

Description: The load of the monitored resource is below the clearing criteria threshold. This event carries only an informative value and can be disabled by the ResourceStateLog property.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE, MRA

Group: Load Admission

Recovery:

No actions are required.

2904 - Diameter/RADIUS protocol is in a busy state

Description: Diameter/RADIUS protocol is in a busy state.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Load Admission

Recovery:

Self-recoverable when load drops below cleanup threshold; if persisted, identify the source of the high Diameter load.

2905 - Diameter/RADIUS protocol is in a normal state

Description: Diameter/RADIUS protocol is in a normal state.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Load Admission

Recovery:

Self-recoverable when load drops below cleanup threshold; if persisted, identify the source of the high RADIUS load.

3100 - Certificate *x* expires in *n* days

Description: The SSL certificate specified by *x* will expire in *n* days. Note: A 90-day SSL certificate is installed by default when a fresh software installation occurs on a system. The expiration of this certificate can cause this trace log code to be generated.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: CMP

Group: Certificate Monitor

Recovery:

1. Delete the expiring SSL certificate using the Platcfg utility to prevent this warning message from being generated again. Platcfg procedures are available in the *Platform Configuration User Guide*.
2. If using https or encryption between servers, create a new certificate using the Platcfg utility.

3101 - Certificate *x* has expired

Description: The SSL certificate specified by *x* has expired. Note: A 90-day SSL certificate is installed by default when a fresh software installation occurs on a system. The expiration of this certificate can cause this trace log code to be generated.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: CMP

Group: Certificate Monitor

Recovery:

1. Delete the expired SSL certificate using the Platcfg utility to prevent this warning message from being generated again. Platcfg procedures are available in the *Platform Configuration User Guide*.
2. If using https or encryption between servers, create a new certificate using the Platcfg utility.

4000 - Policy Action generated critical alarm.

Description: Arbitrary alarm whose cause (and resolution) depends on the policy definition.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: Load Admission

Recovery:

Recovery is based on each individual case.

4001 - Policy Action generated major alarm.

Description: Arbitrary alarm whose cause (and resolution) depends on the policy definition.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: Load Admission

Recovery:

Recovery is based on each individual case.

4002 - Policy Action generated minor alarm.

Description: Arbitrary alarm whose cause (and resolution) depends on the policy definition.

Severity: Error

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: Load Admission

Recovery:

Recovery is based on each individual case.

4003 - CAC: Exception while recreating Tandberg session

Description: An exception occurred in a VoD server.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4004 - CAC: Recreating Tandberg session *id* due to synch operation with *url*

Description: Session is being recreated.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4005 - CAC: Failed to recreate Tandberg session *id* due to sync with *url*

code=*code*, desc=*description*

Description: Failed to recreate Tandberg session *id* due to sync with *url*.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4065 - CAC: Exception while reading local session ID list

Description: This is an internal configuration error.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4066 - CAC: Failed to create CAC session ID *id*

Description: Could not create CAC session ID.

Note: Superceded by even 4200.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4068 - CAC: Exception while sync operation terminated CAC session ID *id*

Description: This is an internal configuration error.

Note: Superceded by even 4201.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4070 - CAC: Failed to release resources for session ID *id*

Description: A gate could not be set from a rejected reserve request.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

If problem persists, contact the Tekelec *Customer Care Center*.

4080 - CAC: Error locating session in CAC database: *error-message*

Description: There was a problem reading the session database.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

If problem persists, contact the Tekelec *Customer Care Center*.

4096 - CAC: Created CAC session ID *id* due to request from VoD server at *server-ip*

Description: The session ID was created successfully.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4144 - CAC: Exception while reserving resources for *id: error-message*

Description: This is an internal configuration error.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4154 - CAC: This blade is now active

Description: This blade is active.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4155 - CAC: This blade is now inactive. Canceling any synchronization in progress

Description: Indicates the primary blade has failed.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Failover to secondary blade. If problem persists, contact the Tekelec *Customer Care Center*.

4156 - CAC: Unknown response from gate delete request

Gate ID = *gate-id* reply type=*reply-type*

Description: There was an internal error while releasing resources.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

If problem persists, contact the Tekelec *Customer Care Center*.

4164 - CAC: Starting synchronization with *server-url*

Description: Synchronization is started between the MPE and a VoD server.

Note: Superceded by even 4205.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4165 - CAC: Synchronization with *server-url* complete

Status: *true/false*

Description: Synchronization is complete. If Status is True, the synchronization completed successfully. If Status is False, the synchronization is aborted after 20 minutes of retries.

Note: Superceded by event 4206.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

If synchronization continues to fail, contact the Tekelec *Customer Care Center*.

4172 - CAC: Locally removing session *id* due to synchronization mismatch with *Seachange/Tandberg* server at *ip-address*

Description: The CAC AM has a session that is not on the VoD server. As a result, the session is removed and all associated resources are released.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4173 - CAC: Locally removing session *id* due to synchronization timeout with *Seachange/Tandberg* server at *ip-address*

Description: Specified session removed due to a synchronization timeout with server with the given address.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4175 - CAC: Requesting removal of session *id* from *Seachange/Tandberg* server at *ip-address* due to synchronization mismatch

Description: Requesting removal of the specified session due to a synchronization mismatch with server with the given address.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4177 - CAC: Rejecting create of session ID *id* from server at *ip-address*: duplicate session

Description: Rejecting create of session ID *id* from server at *ip-address*: duplicate session.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4178 - CAC: Tandberg session ID *id* missing in session list on Tandberg server. Issuing specific query to *url*

Description: Tandberg session ID *id* missing in session list on Tandberg server. Issuing specific query to *url*.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4179 - CAC: Tandberg session ID *id* still missing in session list on Tandberg server at *url* - scheduling removal

Description: Tandberg session ID *id* still missing in session list on Tandberg server at *url* - scheduling removal.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4180 - CAC: Keepalive status request from Tandberg server at *ip-address*

Description: Keepalive status request from Tandberg server at *ip-address*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4181 - CAC: Session list status request from *Seachange/Tandberg* server at *ip-address*

Description: Session list status request from *Seachange/Tandberg* server at *ip-address*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4182 - CAC: Session detail status request from Tandberg server at *ip-address* for session ID *id*

Description: Session detail status request from Tandberg server at *ip-address* for session ID *id*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4183 - CAC: Version status request from Tandberg server at *ip-address*

Description: Version status request from Tandberg server at *ip-address*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4184 - CAC: *Seachange/Tandberg* reserve of session *id* on *ip-address* complete

status: *status*, duration: *time* ms

Description: A session was successfully reserved.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4185 - CAC: *Seachange/Tandberg* release of session *id* complete

status: *status*, duration: *time* ms

Description: A session was successfully released.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4188 - CAC: No keepalive response from Tandberg server at *url*

Description: No keepalive response from Tandberg server at *url*.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4189 - CAC: Exception while releasing session *id* from Tandberg server

Description: Exception while releasing session *id* from Tandberg server.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4190 - CAC: Tandberg server requesting release of session ID *id*

Code=*code*, Text=*desc*

Description: Tandberg server requesting release of session ID *id*, Code=*code*, Text=*desc*

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4191 - CAC: No version status response from Tandberg server at *url*

Description: No version status response from Tandberg server at *url*.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4192 - CAC: Version report from Tandberg server at *url*

software: *sw-version*, interface: *int-version*

Description: Version report from Tandberg server at *url*, software: *sw-version*, interface: *int-version*

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4193 - CAC: Invalid version report from Tandberg server at *url*

Description: Invalid version report from Tandberg server at *url*

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4194 - CAC: Sending keepalive request to Tandberg server at *url*

Description: Sending keepalive request to Tandberg server at *url*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4195 - CAC: Received keepalive response from Tandberg server at *url*

code=*code*, text=*status*, duration *duration* ms

Description: Received a KeepAlive response from a Tandberg server with a status code of *code* and a status description of *status*.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4196 - CAC: Sync mismatch with *Seachange/Tandberg* server at *ip-address*: VoD server has *n* sessions missing on MPE

Description: Sync mismatch with *Seachange/Tandberg* server at *ip-address*: VoD server has *n* sessions missing on MPE

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4200 - CAC: Failed to create CAC session ID *id* from VoD Server at *server-ip* for subscriber IP *sub-ip: status*

Description: Could not create CAC session ID.

Note: Supercedes event 4066.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4201 - CAC: Exception while *Seachange/Tandberg* sync operation with *url* terminated CAC session ID *id*

Description: This is an internal configuration error.

Note: Supercedes event 4068.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4203 - CAC: Error requesting session list from *Seachange/Tandberg* server at *url*

Description: This is an internal configuration error.

Note: Supercedes event 4159.

Severity: Warn

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

Contact the Tekelec *Customer Care Center*.

4205 - CAC: Starting synchronization with *Seachange/Tandberg* server at *url*

Description: Synchronization has started between the MPE device and a VoD server.

Note: Supercedes event 4164.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4206 - CAC: Synchronization with *Seachange/Tandberg* server at *url* complete

Status = True/False

Description: Synchronization is complete. If Status is True, the synchronization completed successfully. If Status is False, the synchronization is aborted after 20 minutes of retries.

Note: Supercedes event 4165.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

If synchronization continues to fail, contact the Tekelec *Customer Care Center*.

4207 - CAC: Max sync failures with *Seachange/Tandberg* server at *ip-address*: removing *n* sessions

Description: Synchronization timed out; *n* sessions were removed from the indicated server at the indicated IP address.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4208 - CAC: *Seachange/Tandberg* reserve of duplicate session *id* on *ip-address* complete: status *status*, duration *time* ms

Description: A session with a duplicate ID was successfully reserved.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: CAC

Recovery:

No action required.

4300 - RC *ip-address* Unreachable

Description: The CMP to MPE connection has failed.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: Load Admission

Recovery:

Policy execution INFO trace log

4301 - RC *ip-address* Reachable

Description: The CMP to MPE connection has been restored.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: Load Admission

Recovery:

Policy execution INFO trace log

4302 - RC *ip-address* Unreachable - operation: *operation*

Description: The CMP to MPE connection failed during the specified operation.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE

Group: Load Admission

Recovery:

1. Policy execution INFO trace log.
2. Contact the Tekelec *Customer Care Center*.

4550 - Policy Trace *name*: *message*

Description: Policy generated Warning level Trace Log notification.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy execution INFO trace log

4551 - Policy Trace *name*: *message*

Description: Policy generated Info level Trace Log notification.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy execution WARN trace log

4552 - Policy Trace *name*: *message*

Description: Policy generated Debug level Trace Log notification.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy execution DEBUG trace log

4560 - Policy Action Trace: *message*

Description: Policy Action generated Emergency Trace Log notification.

Severity: Emergency

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log EMERGENCY action

4561 - Policy Action Trace: *message*

Description: Policy Action generated Alert Trace Log notification.

Severity: Alert

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log ALERT action

4562 - Policy Action Trace: *message*

Description: Policy Action generated Critical Trace Log notification.

Severity: Critical

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log CRITICAL action

4563 - Policy Action Trace: *message*

Description: Policy Action generated Error Trace Log notification.

Severity: Error

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log ERROR action

4564 - Policy Action Trace: *message*

Description: Policy Action generated Warning Trace Log notification.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log WARNING action

4565 - Policy Action Trace: *message*

Description: Policy Action generated Notice Trace Log notification

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log NOTICE action

4566 - Policy Action Trace: *message*

Description: Policy Action generated Info Trace Log notification.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log INFO action

4567 - Policy Action Trace: *message*

Description: Policy Action generated Debug Trace Log notification.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Load Admission

Recovery:

Policy generated trace log DEBUG action

4600 - MPE or MRA rejects a secondary connection

Description: A Secondary connection has been rejected due to a Primary connection already existing from the same Diameter identity. This could indicate a split brain situation at the remote identity.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Georedundancy

Recovery:

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. If alarm persists, contact the Tekelec *Customer Care Center*.

4601 - MPE or MRA reverts from a secondary connection to a primary connection

Description: A connection has reverted from a Secondary connection to a Primary connection. While this could happen normally during a remote failover, it could also indicate a potential split brain situation at the remote cluster.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: MPE, MRA

Group: Georedundancy

Recovery:

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. If alarm persists, contact the Tekelec *Customer Care Center*.

4602 - More than one server in a cluster is Active at a time

Description: Multiple Active servers have been detected in the same cluster; this indicates that the cluster is in Split Brain.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: CMP

Group: Georedundancy

Recovery:

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. Contact the Tekelec *Customer Care Center*.

4603 - Max primary site failure threshold reached

Description: Number of failed MPE Primary Sites has reached the threshold.

Severity: Warning

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: CMP

Group: Georedundancy

Recovery:

1. When the failure count drops below the threshold value and stays below the threshold for 30 seconds, the alarm is cleared. (The 30 seconds delay prevents the alarm from being cleared too soon.)
2. If alarm doesn't clear automatically, contact the Tekelec *Customer Care Center*.

4604 - Policy Cluster Offline Failure

Description: An MPE/MRA policy cluster is offline. None of the servers in this cluster are available (Active, Standby, or Spare).

Severity: Critical

Notification: Trace Log

Alarm: Yes

Trap: Yes

Server: CMP

Group: Georedundancy

Recovery:

1. When a server comes online (in Active, Standby, or Spare state), the alarm is cleared. Please check whether all servers are powered down or rebooted at that time.
2. If alarm doesn't clear automatically, contact the Tekelec *Customer Care Center*.

4610 - *Sh Connections operation* Successful for *MPEs' name*, Failed for *MPEs' name*

Description: The CMP performed a global operation to enable (or disable) Sh on all MPE's with the results as specificed (MPE's for which it was successful are listed; MPE's for which the operation failed are also listed).

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: CMP

Group: Sh

Recovery:

If the operations failed for some MPEs then it can be retried. If repeated attempts fail then there may be other management issues with the associated MPEs and connectivity to those devices should be verified.

4700 - Upgrade Manager command return message: *message*

Description: Upgrade Manager executes command on remote server and gets the return message, then generates the Info Trace Log notification.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: CMP

Group: Upgrade

Recovery:

No action required.

10000 - ADS: Analytics Data Stream connection to *Analytics Client ID* has been established for Channel: *Channel Type, ex Policy Event* Version: *ADS Interface Version* Connection established to the MPE from an Analytics client

Description: Connection established to the MPE from an Analytics client.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: ADS

Recovery:

No action required.

10001 - ADS: Analytics Data Stream connection to *Analytics Client ID* was closed

Description: Connection between the MPE and Analytics client was closed.

Severity: Notice

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: ADS

Recovery:

No action required.

10002 - ADS: Lost Analytics Data Stream connection to *Analytics Client ID*

Description: Connection between MPE and Analytics client was closed due to error.

Severity: Warning

Notification: Trace Log

Alarm: Yes - 78000

Trap: No

Server: MPE

Group: ADS

Recovery:

No action required.

10003 - ADS: Error processing Analytics Data Stream message received from *Analytics Client ID*

Description: Analytics Data Stream Request from Analytics Client resulted in error.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: ADS

Recovery:

No action required.

10004 - ADS: Error sending Analytics Data Stream message to *Analytics Client ID*

Description: Error occurred while sending Analytics Data Stream message from the MPE.

Severity: Debug

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: ADS

Recovery:

No action required.

10005 - ADS: Analytics Data Stream encountered an error

Description: Error occurred during Analytics Data Stream processing.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: ADS

Recovery:

No action required.

10006 - SY: Received notification from *Sy Identity* message: *Diameter message*

Description: Indicates an SNR was received from the OCS and provides the message details.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SY

Recovery:

No action required.

10007 - SY: Peer Realm is undefined

Description: Undefined Realm in Sy configuration.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SY

Recovery:

Check the configured Realm for the connection.

10008 - SY: Primary address is undefined

Description: Undefined Address in Sy configuration.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SY

Recovery:

Check the configured Address for the connection.

10009 - SY: Searching *Sy Identity* for subscriber: *Subscriber IDs*

Description: Indicates a new SLR search has been started for the given subscriber.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SY

Recovery:

No actions required.

10010 - SY: Search results from peer *Sy Identity* for subscriber *Subscriber IDs* are: *Policy Counter values*

Description: Indicates a successful SLR/SLA lookup and details the contents.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SY

Recovery:

No actions required.

10012 - SY: Search failure on *Sy Identity*: *Diameter Error Code* subscriber *Subscriber IDs*

Description: Lookups that result in a failure response in the SLA that occur during a Sy SLR lookup with the OCS.

Severity: Warning

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: SY

Recovery:

No actions required.

Chapter 4

Alarms and Events

Topics:

- *Alarms formatting information.....165*
- *Alarm and Event Severity Levels.....165*
- *Platform (31000-32700).....165*
- *QBus Platform (70000-70999).....205*
- *Policy Server (71000-89999).....213*

Alarms and Events provides general alarm and 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.

Note: If you encounter an alarm not in this document, contact the Tekelec *Customer Care Center*.

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 Event that has occurred.
- Description: describes the reason for the Event
- Default Severity: the severity of the alarm. This severity may vary, depending on user-defined and specific application settings.
- OID: alarm identifier that appears in SNMP traps
- Alarm ID: alarm identifier used internally to Tekelec
- Recovery: provides any necessary steps for correcting or preventing the alarm

Alarm and Event Severity Levels

Alarms can be one of three severity levels:

1. Critical
2. Major
3. Minor

Events note the occurrence of an expected condition and are logged in the Trace Log. Events have these severity levels:

1. Emergency
2. Alert
3. Critical
4. Error
5. Warning
6. Notice
7. Info
8. Debug

Platform (31000-32700)

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

31000 - S/W Fault

Alarm Type: SW

Description: Program impaired by s/w fault

Default Severity: Minor

OID: comcolSwFaultNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact Tekelec *Customer Care Center*.

31001 - S/W Status

Alarm Type: SW

Description: Program status

Default Severity: Info

OID: comcolSWStatusNotify

Recovery:

No action required.

31002 - Process Watchdog Failure

Alarm Type: SW

Description: Process watchdog timed out

Default Severity: Minor

OID: comcolProcWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact Tekelec *Customer Care Center*.

31003 - Thread Watchdog Failure

Alarm Type: SW

Description: Thread watchdog timed out

Default Severity: Minor

OID: comcolThreadWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact Tekelec *Customer Care Center*.

31100 - DB Replication Fault

Alarm Type: SW

Description: The DB replication process (inetsync) is impaired by a s/w fault

Default Severity: Minor

OID: comcolDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact Tekelec *Customer Care Center*.

31101 - DB Replication To Slave Failure

Alarm Type: REPL

Description: DB replication to a slave DB has failed

Default Severity: Minor

OID: comcolDbRepToSlaveFailureNotify

Recovery:

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31102 - DB Replication From Master Failure

Alarm Type: REPL

Description: DB replication from a master DB has failed

Default Severity: Minor

OID: comcolDbRepFromMasterFailureNotify

Recovery:

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31103 - DB Replication Update Fault

Alarm Type: REPL

Description: DB replication process cannot apply update to DB

Default Severity: Minor

OID: comcolDbRepUpdateFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact Tekelec *Customer Care Center*.

31104 - DB Replication Latency Over Threshold

Alarm Type: REPL

Description: DB replication latency has exceeded thresholds

Default Severity: Minor

OID: comcolDbRepLatencyNotify

Recovery:

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

31105 - DB Merge Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolDbMergeFaultNotify

Recovery:

1. Export event history for the given server and inetmerge task.
2. Contact Tekelec *Customer Care Center*.

31106 - DB Merge To Parent Failure

Alarm Type: COLL

Description: DB merging to the parent Merge Node has failed

Default Severity: Minor

OID: comcolDbMergeToParentFailureNotify

Recovery:

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31107 - DB Merge From Child Failure

Alarm Type: COLL

Description: DB merging from a child Source Node has failed

Default Severity: Minor

OID: comcolDbMergeFromChildFailureNotify

Recovery:

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31108 - DB Merge Latency Over Threshold

Alarm Type: COLL

Description: DB Merge latency has exceeded thresholds

Default Severity: Minor

OID: comcolDbMergeLatencyNotify

Recovery:

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

31109 - Topology Config Error

Alarm Type: DB

Description: Topology is configured incorrectly

Default Severity: Minor

OID: comcolTopErrorNotify

Recovery:

1. This alarm may occur during initial installation and configuration of a server. No action is necessary at that time.
2. If this alarm occurs after successful initial installation and configuration of a server, contact the Tekelec *Customer Care Center*.

31110 - DB Audit Fault

Alarm Type: SW

Description: The DB audit process (iaudit) is impaired by a s/w fault

Default Severity: Minor

OID: comcolDbAuditFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact Tekelec *Customer Care Center*.

31111 - DB Merge Audit in Progress

Alarm Type: COLL

Description: DB Merge Audit between mate nodes in progress

Default Severity: Minor

OID: comcolDbMergeAuditNotify

Recovery:

No action required.

31112 - DB Replication Update Log Transfer Timed Out

Alarm Type: REPL

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

Default Severity: Minor

OID: comcolDbRepUpLogTransTimeoutNotify

Recovery:

No action required. Contact Tekelec *Customer Care Center* if this occurs frequently.

31113 - DB Replication Manually Disabled

Alarm Type: REPL

Description: Replication Manually Disabled

Default Severity: Minor

OID: comcolDbReplicationManuallyDisabledNotify

Recovery:

No action required.

31114 - DB Replication over SOAP has failed

Alarm Type: REPL

Description: DB replication of configuration data via SOAP has failed

Default Severity: Minor

OID: comcolDbReplicationSoapFaultNotify

Recovery:

1. Check network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the Tekelec *Customer Care Center*.

31115 - DB Service Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolDbServiceFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact Tekelec *Customer Care Center*.

31116 - Excessive Shared Memory

Alarm Type: MEM

Description: The amount of shared memory consumed exceeds configured thresholds

Default Severity: Major

OID: comcolExcessiveSharedMemoryConsumptionNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31117 - Low Disk Free

Alarm Type: DISK

Description: The amount of free disk is below configured thresholds

Default Severity: Major

OID: comcolLowDiskFreeNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact Tekelec *Customer Care Center*.

31118 - DB Disk Store Fault

Alarm Type: DISK

Description: Writing the database to disk failed

Default Severity: Minor

OID: comcolDbDiskStoreFaultNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.

2. If there are no files known to be unneeded, contact Tekelec *Customer Care Center*.

31119 - DB Updatelog Overrun

Alarm Type: DB

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

Default Severity: Minor

OID: comcolDbUpdateLogOverrunNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31120 - DB Updatelog Write Fault

Alarm Type: DB

Description: A DB change cannot be stored in the updatelog

Default Severity: Minor

OID: comcolDbUpdateLogWriteFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31121 - Low Disk Free Early Warning

Alarm Type: DISK

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

Default Severity: Minor

OID: comcolLowDiskFreeEarlyWarningNotify

Recovery:

1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
2. If there are no files known to be unneeded, contact Tekelec *Customer Care Center*.

31122 - Excessive Shared Memory Early Warning

Alarm Type: MEM

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

Default Severity: Minor

OID: comcolExcessiveSharedMemoryConsumptionEarlyWarnNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31123 - DB Replication Audit Complete

Alarm Type: REPL

Description: DB replication audit (command) completed

Default Severity: Info

OID: comcolDbRepAuditCompleteNotify

Recovery:

No action required.

31124 - DB Replication Audit Command Error

Alarm Type: REPL

Description: A DB replication audit command detected errors

Default Severity: Minor

OID: comcolDbRepAuditCmdErrNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31125 - DB Durability Degraded

Alarm Type: REPL

Description: DB durability has dropped below configured durability level

Default Severity: Major

OID: comcolDbDurabilityDegradedNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, contact Tekelec *Customer Care Center*.

31126 - Audit Blocked

Alarm Type: REPL

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

Default Severity: Major

OID: comcolAuditBlockedNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31130 - Network Health Warning

Alarm Type: NET

Description: Network health issue detected

Default Severity: Minor

OID: comcolNetworkHealthWarningNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, contact Tekelec *Customer Care Center*.

31140 - DB Perl Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolDbPerlFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31145 - DB SQL Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolDbSQLFaultNotify

Recovery:

1. Export event history for the given server, and Imysqld task.
2. Contact Tekelec *Customer Care Center*.

31146 - DB Mastership Fault

Alarm Type: SW

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

Default Severity: Major

OID: comcolDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. Contact Tekelec *Customer Care Center*.

31147 - DB UpSyncLog Overrun

Alarm Type: SW

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

Default Severity: Minor

OID: comcolDbUpSyncLogOverrunNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31148 - DB Lock Error Detected

Alarm Type: DB

Description: DB lock integrity error detected -- 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.

Default Severity: Minor

OID: comcolDbLockErrorNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31200 - Process Management Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolProcMgmtFaultNotify

Recovery:

1. Export event history for the given server, all processes.
2. Contact Tekelec *Customer Care Center*.

31201 - Process Not Running

Alarm Type: PROC

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

Default Severity: Major

OID: comcolProcNotRunningNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31202 - Unkillable Zombie Process

Alarm Type: PROC

Description: A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.

Default Severity: Major

OID: comcolProcZombieProcessNotify

Recovery:

1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. Contact Tekelec *Customer Care Center*.

31206 - Process Mgmt Monitoring Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolProcMgmtMonFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31207 - Process Resource Monitoring Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolProcResourceMonFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31208 - IP Port Server Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolPortServerFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31209 - Hostname Lookup Failed

Alarm Type: SW

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

Default Severity: Minor

OID: comcolHostLookupFailedNotify

Recovery:

1. This typically indicate a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, contact Tekelec *Customer Care Center*.

31213 - Process Scheduler Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolProcSchedulerFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31214 - Scheduled Process Fault

Alarm Type: PROC

Description: A scheduled process cannot be executed or abnormally terminated

Default Severity: Minor

OID: comcolScheduleProcessFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31215 - Process Resources Exceeded

Alarm Type: SW

Description: A process is consuming excessive system resources

Default Severity: Minor

OID: comcolProcResourcesExceededFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31216 - SysMetric Configuration Error

Alarm Type: SW

Description: A SysMetric Configuration table contains invalid data

Default Severity: Minor

OID: comcolSysMetricConfigErrorNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31220 - HA Config Monitor Fault

Alarm Type: SW

Description: The HA manager (cmha) is impaired by a s/w fault

Default Severity: Minor

OID: comcolHaCfgMonitorFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31221 - HA Alarm Monitor Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolHaAlarmMonitorFaultNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31222 - HA Not Configured

Alarm Type: HA

Description: High availability is disabled due to system configuration

Default Severity: Minor

OID: comcolHaNotConfiguredNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31223 - HA Heartbeat Transmit Failure

Alarm Type: HA

Description: The high availability monitor failed to send heartbeat

Default Severity: Major

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, contact Tekelec *Customer Care Center*.

31224 - HA Configuration Error

Alarm Type: HA

Description: High availability configuration error

Default Severity: Major

OID: comcolHaCfgErrorNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

31225 - HA Service Start Failure

Alarm Type: HA

Description: The high availability service failed to start

Default Severity: Major

OID: comcolHaSvcStartFailureNotify

Recovery:

1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, contact Tekelec *Customer Care Center*.

31226 - HA Availability Status Degraded

Alarm Type: HA

Description: The high availability status is degraded due to raised alarms

Default Severity: Major

OID: comcolHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact Tekelec *Customer Care Center*.

31227 - HA Availability Status Failed

Alarm Type: HA

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

Default Severity: Critical

OID: comcolHaAvailFailedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact Tekelec *Customer Care Center*.

31228 - HA Standby Server Offline

Alarm Type: HA

Description: HA Standby Server Offline

Default Severity: Critical

OID: comcolHaStandbyOfflineNotify

Recovery:

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

31229 - HA Score Changed

Alarm Type: HA

Description: High availability health score changed

Default Severity: Info

OID: comcolHaScoreChangeNotify

Recovery:

Status message - no action required.

31230 - Recent Alarm Processing Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolRecAlarmEvProcFaultNotify

Recovery:

1. Export event history for the given server and raclerk task.
2. Contact Tekelec *Customer Care Center*.

31231 - Platform Alarm Agent Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolPlatAlarmAgentNotify

Recovery:

Contact Tekelec *Customer Care Center*.

31232 - HA Late Heartbeat Warning

Alarm Type: HA

Description: High availability server has not received a heartbeat within the configured interval

Default Severity: Minor

OID: comcolHaLateHeartbeatWarningNotify

Recovery:

No action required; this is a warning and can be due to transient conditions. If there continues to be no heartbeat from the server, alarm 31228 occurs.

31240 - Measurements Collection Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolMeasCollectorFaultNotify

Recovery:

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

2. Contact Tekelec *Customer Care Center*.

31250 - RE Port Mapping Fault

Alarm Type: SW

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

Default Severity: Minor

OID: comcolRePortMappingFaultNotify

Recovery:

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

31260 - DB SNMP Agent

Alarm Type: SW

Description: The DB SNMP agent (snmpIdbAgent) is impaired by a s/w fault

Default Severity: Minor

OID: comcolDbSnmpAgentNotify

Recovery:

1. Export event history for the given server and all processes.
2. Contact Tekelec *Customer Care Center*.

31270 - Logging Output

Alarm Type: SW

Description: Logging output set to Above Normal

Default Severity: Minor

OID: comcolLoggingOutputNotify

Recovery:

Extra diagnostic logs are being collected, potentially degrading system performance. Contact Tekelec *Customer Care Center*.

31280 - HA Active to Standby Transition

Alarm Type: HA

Description: HA active to standby activity transition

Default Severity: Info

OID: comcolActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31281 - HA Standby to Active Transition

Alarm Type: HA

Description: HA standby to active activity transition

Default Severity: Info

OID: comcolStandbyToActiveTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31282 - HA Management Fault

Alarm Type: HA

Description: The HA manager (cmha) is impaired by a s/w fault.

Default Severity: Minor

OID: comcolHaMgmtFaultNotify

Recovery:

Export event history for the given server and cmha task, then contact Tekelec *Customer Care Center*.

31283 - HA Server Offline

Alarm Type: HA

Description: High availability server is offline

Default Severity: Critical

OID: comcolHAServerOfflineNotify

Recovery

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

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Type: HA

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

Default Severity: Minor

OID: comcolHARemoteHeartbeatWarningNotify

Recovery

1. No action required; this is a warning and can be due to transient conditions. The remote subscriber will move to another server in the cluster.
2. If there continues to be no heartbeat from the server, contact Tekelec *Customer Care Center*.

31290 - HA Process Status

Alarm Type: HA

Description: HA manager (cmha) status

Default Severity: Info

OID: comcolHaProcessStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31291 - HA Election Status

Alarm Type: HA

Description: HA DC Election status

Default Severity: Info

OID: comcolHAElectionStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31292 - HA Policy Status

Alarm Type: HA

Description: HA Policy plan status

Default Severity: Info

OID: comcolHaPolicyStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31293 - HA Resource Link Status

Alarm Type: HA

Description: HA Resource Agent Link status

Default Severity: Info

OID: comcolHaRaLinkStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31294 - HA Resource Status

Alarm Type: HA

Description: HA Resource registration status

Default Severity: Info

OID: comcolHaResourceStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31295 - HA Action Status

Alarm Type: HA

Description: HA Resource action status

Default Severity: Info

OID: comcolHaActionStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31296 - HA Monitor Status

Alarm Type: HA

Description: HA Monitor action status

Default Severity: Info

OID: comcolHaMonitorStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31297 - HA Resource Agent Info

Alarm Type: HA

Description: HA Resource Agent application information

Default Severity: Info

OID: comcolHaRaInfoNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

31298 - HA Resource Agent Detail

Alarm Type: HA

Description: HA Resource Agent application detailed information

Default Severity: Info

OID: comcolHaRaDetailNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact Tekelec *Customer Care Center*.

32113 - Uncorrectable ECC Memory Error

Alarm Type: PLAT

Description: Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Default Severity: Critical

OID: tpdEccUncorrectableError

Recovery

Contact the Tekelec *Customer Care Center* to request hardware replacement.

32114 - SNMP Get Failure

Alarm Type: PLAT

Description: SNMP Get Failure -- The server failed to receive SNMP information from the switch.

Default Severity: Critical

OID: tpdSNMPGetFailure

Within this trap is one bind variable, the OID of which is 1.3.6.1.2.1.1.5 <sysname>, where <sysname> is the name of the switch where the failure occurred.

Recovery

1. Use the following command to verify the switch is active: `ping switch1A/B` (this requires command line access).
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32300 – Server Fan Failure

Alarm Type: PLAT

Description: Server Fan Failure -- 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.

Default Severity: Major

OID: tpdFanError

Recovery

Contact the Tekelec *Customer Care Center*.

32301 - Server Internal Disk Error

Alarm Type: PLAT

Description: Server Internal Disk Error -- 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.

Default Severity: Major

OID: tpdIntDiskError

Recovery

Contact the Tekelec *Customer Care Center*.

32302 – Server RAID Disk Error

Alarm Type: PLAT

Description: Server RAID Disk Error -- This alarm indicates that the offboard storage server had a problem with its hardware disks.

Default Severity: Major

OID: tpdRaidDiskError

Recovery

Contact the Tekelec *Customer Care Center*.

32303 - Server Platform Error

Alarm Type: PLAT

Description: Server Platform Error - This alarm indicates an error such as a corrupt system configuration or missing files.

Default Severity: Major

OID: tpdPlatformError

Recovery

Contact the Tekelec *Customer Care Center*.

32304 - Server File System Error

Alarm Type: PLAT

Description: Server File System Error -- This alarm indicates unsuccessful writing to at least one of the server's file systems.

Default Severity: Major

OID: tpdFileSystemError

Recovery

Contact the Tekelec *Customer Care Center*.

32305 - Server Platform Process Error

Alarm Type: PLAT

Description: Server Platform Process Error -- 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.

Default Severity: Major

OID: tpdPlatProcessError

Recovery

Contact the Tekelec *Customer Care Center*.

32307 - Server Swap Space Shortage Error

Alarm Type: PLAT

Description: Server Swap Space Shortage Error -- 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.

Default Severity: Major

OID: tpdSwapSpaceShortageError

Recovery

Contact the Tekelec *Customer Care Center*.

32308 - Server Provisioning Network Error

Alarm Type: PLAT

Description: Server Provisioning Network Error -- This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly. The eth1 interface is at the upper right port on the rear of the server on the EAGLE backplane.

Default Severity: Major

OID: tpdProvNetworkError

Recovery

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

32312 - Server Disk Space Shortage Error

Alarm Type: PLAT

Description: Server Disk Space Shortage Error -- This alarm indicates that one of the following conditions has occurred:

- A filesystem has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the filesystem.
- More than 90% of the total number of available files have been allocated on the filesystem.
- A filesystem has a different number of blocks than it had when installed.

Default Severity: Major

OID: tpdDiskSpaceShortageError

Recovery

Contact the Tekelec *Customer Care Center*.

32313 - Server Default Route Network Error

Alarm Type: PLAT

Description: Server Default Route Network Error -- This alarm indicates that the default network route of the server is experiencing a problem.

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

Default Severity: Major

OID: tpdDefaultRouteNetworkError

Recovery

Contact the Tekelec *Customer Care Center*.

32314 - Server Temperature Error

Alarm Type: PLAT

Description: Server Temperature Error -- The internal temperature within the server is unacceptably high.

Default Severity: Major

OID: tpdTemperatureError

Recovery

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

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

3. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32315 – Server Mainboard Voltage Error

Alarm Type: PLAT

Description: Server Mainboard Voltage Error -- 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.

Default Severity: Major

OID: tpdServerMainboardVoltageError

Recovery

Contact the Tekelec *Customer Care Center*.

32316 – Server Power Feed Error

Alarm Type: PLAT

Description: Server Power Feed Error -- 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.

Default Severity: Major

OID: tpdPowerFeedError

Recovery

1. Verify that all the server power feed cables to the server that is reporting the error are securely connected.
2. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
3. Follow the power feed to its connection on the power source. Ensure that the power source is ON and that the power feed is properly secured.
4. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
5. If the power source is functioning properly and the wires are all secure, have an electrician check the voltage on the power feed.
6. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
7. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32317 - Server Disk Health Test Error

Alarm Type: PLAT

Description: Server Disk Health Test Error -- Either the hard drive has failed or failure is imminent.

Default Severity: Major

OID: tpdDiskHealthError

Recovery

1. Perform the recovery procedures for the other alarms that accompany this alarm.
2. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32318 - Server Disk Unavailable Error

Alarm Type: PLAT

Description: Server Disk Unavailable Error -- 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.

Default Severity: Major

OID: tpdDiskUnavailableError

Recovery

Contact the Tekelec *Customer Care Center*.

32320 – Device Interface Error

Alarm Type: PLAT

Description: Device Interface Error -- This alarm indicates that the IP bond is either not configured or down.

Default Severity: Major

OID: tpdDeviceIfError

Recovery

Contact the Tekelec *Customer Care Center*.

32321 – Correctable ECC memory error

Alarm Type: PLAT

Description: Correctable ECC Memory Error -- 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.

Default Severity: Major

OID: tpdEccCorrectableError

Recovery

No recovery necessary. If the condition persists, contact the Tekelec *Customer Care Center* to request hardware replacement.

32322 – Power Supply A error

Alarm Type: PLAT

Description: Power Supply A Error -- This alarm indicates that power supply 1 (feed A) has failed.

Default Severity: Major

OID: tpdPowerSupply1Error

Recovery

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32323 – Power Supply B Error

Alarm Type: PLAT

Description: Power Supply B Error -- This alarm indicates that power supply 2 (feed B) has failed.

Default Severity: Major

OID: tpdPowerSupply2Error

Recovery

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

32324 – Breaker panel Feed Error

Alarm Type: PLAT

Description: Breaker Panel Feed Error -- This alarm indicates that the server is not receiving information from the breaker panel relays.

Default Severity: Major

OID: tpdBrkPnlFeedError

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, call the Tekelec *Customer Care Center* to request that the breaker panel be replaced.

32325 – Breaker Panel Breaker Error

Alarm Type: PLAT

Description: Breaker Panel Breaker Error -- This alarm indicates that a power fault has been identified by the breaker panel.

Default Severity: Major

OID: tpdBrkPnlBreakerError

Recovery

1. Verify that the same alarm is displayed by multiple servers:
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by multiple servers, go to the next step.
2. Look at the breaker panel assignments and verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.
3. Check the BRK FAIL LEDs for BUS A and for BUS B.
   - If one of the BRK FAIL LEDs is illuminated Red, then one or more of the respective Input Breakers has tripped. (A tripped breaker is indicated by the toggle located in the center position.) Perform the following steps to repair this issue:

   a) For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.
   b) After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, contact the Tekelec *Customer Care Center*.

   - If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, continue with the next step.
4. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32326 – Breaker Panel Monitoring Error

Alarm Type: PLAT

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

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

- 32324-Breaker Panel Feed Error or
- 32325-Breaker Panel Breaker Error

until the Breaker Panel Monitoring Error has been corrected.

Default Severity: Major

OID: tpdBrkPnlMntError

Recovery

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

- If this alarm is displayed by multiple servers, go to the next step.

2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).
3. If the alarm has not been cleared, contact the Tekelec *Customer Care Center*.

32327 – Server HA Keepalive Error

Alarm Type: PLAT

Description: Server HA Keepalive Error -- This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Default Severity: Major

OID: tpdHaKeepaliveError

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. Contact the Tekelec *Customer Care Center*.

32331 – HP disk problem

Alarm Type: TPD

Description: HP disk problem -- 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.

Default Severity: Major

OID: tpdHpDiskProblemNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32332 – HP Smart Array controller problem

Alarm Type: PLAT

Description: HP Smart Array controller problem -- 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.

Default Severity: Major

OID: tpdHpDiskCtrlrProblemNotify

Recovery

Contact the Tekelec *Customer Care Center*.

32333 – HP hpacucliStatus utility problem

Alarm Type: PLAT

Description: HP hpacucliStatus utility problem -- This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus daemon is either not running, or hung.

Default Severity: Major

OID: tpdHPACUCLIProblem

Recovery

Contact the Tekelec *Customer Care Center*.

32335 - Switch Link Down Error

Alarm Type: PLAT

Description: Swith Link Down Error -- The link is down.

Default Severity: Major

OID: tpdSwitchLinkDownError

Within this trap are two bind variables, the OIDs of which are:

- 1.3.6.1.2.1.1.5 <sysname>, where <sysname> is the name of the switch where the failure occurred.
- 1.3.6.1.2.1.2.2.1.1 <link index>, where <link index> is the index of the failed link.

Recovery

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, contact the Tekelec *Customer Care Center*, who should verify port settings on both the server and the switch.

32336 – Half open socket limit

Alarm Type: PLAT

Description: Half open socket limit -- 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.

Default Severity: Major

OID: tpdHalfOpenSockLimit

Recovery

Contact the Tekelec *Customer Care Center*.

32500 – Server Disk Space Shortage Warning

Alarm Type: PLAT

Description: Server Disk Space Shortage Warning -- 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.

Default Severity: Minor

OID: tpdDiskSpaceShortageWarning

Recovery

Contact the Tekelec *Customer Care Center*.

32501 – Server Application Process Error

Alarm Type: PLAT

Description: Server Application Process Error -- 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.

Default Severity: Minor

OID: tpdApplicationProcessError

Recovery

Contact the Tekelec *Customer Care Center*.

32502 – Server Hardware Configuration Error

Alarm Type: PLAT

Description: Server Hardware Configuration Error -- This alarm indicates that one or more of the server's hardware components are not in compliance with Tekelec specifications (refer to the appropriate hardware manual).

Default Severity: Minor

OID: tpdHardwareConfigError

Recovery

Contact the Tekelec *Customer Care Center*.

32505 – Server Swap Space Shortage Warning

Alarm Type: PLAT

Description: Server Swap Space Shortage Warning -- 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.

Default Severity: Minor

OID: tpdSwapSpaceShortageWarning

Recovery

Contact the Tekelec *Customer Care Center*.

32506 – Server Default Router not Defined

Alarm Type: PLAT

Description: Server Default Router not Defined -- This alarm indicates that the default network route is either not configured or the current configuration contains an invalid IP address or hostname.

Default Severity: Minor

OID: tpdDefaultRouteNotDefined

Recovery

Contact the Tekelec *Customer Care Center*.

32507 – Server Temperature Warning

Alarm Type: PLAT

Description: Server Temperature Warning -- 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.

Default Severity: Minor

OID: tpdTemperatureWarning

Recovery

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

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

3. 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.

4. If the problem has not been resolved, contact the Tekelec *Customer Care Center*.

32508 – Server Core File Detected

Alarm Type: PLAT

Description: Server Core File Detected -- This alarm indicates that an application process has failed and debug information is available.

Default Severity: Minor

OID: tpdCoreFileDetected

Recovery

Contact the Tekelec *Customer Care Center*.

32509 – Server NTP Daemon Not Synchronized

Alarm Type: PLAT

Description: Server NTP Daemon Not Synchronized -- This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Default Severity: Minor

OID: tpdNTPDeamonNotSynchronized

Recovery

Contact the Tekelec *Customer Care Center*.

32510 – CMOS Battery Voltage Low

Alarm Type: PLAT

Description: CMOS Battery Voltage Low -- 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.

Default Severity: Minor

OID: tpdCMOSBatteryVoltageLow

Recovery

Contact the Tekelec *Customer Care Center*.

32511 – Server Disk Self Test Warning

Alarm Type: PLAT

Description: Server Disk Self Test Warning -- A non-fatal disk issue (such as a sector cannot be read) exists.

Default Severity: Minor

OID: tpdSmartTestWarn

Recovery

Contact the Tekelec *Customer Care Center*.

32512 – Device Warning

Alarm Type: PLAT

Description: Device Warning -- 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.

Default Severity: Minor

OID: tpdDeviceWarn

Recovery

Contact the Tekelec *Customer Care Center*.

32513 – Device Interface Warning

Alarm Type: PLAT

Description: Device Interface Warning -- This alarm can be generated by either an SNMP trap or an IP bond error.

Default Severity: Minor

OID: tpdDeviceIfWarn

Recovery

Contact the Tekelec *Customer Care Center*.

32514 – Server Reboot Watchdog Initiated

Alarm Type: PLAT

Description: Server Reboot Watchdog Initiated -- 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.

Default Severity: Minor

OID: tpdWatchdogReboot

Recovery

Contact the Tekelec *Customer Care Center*.

32515 – Server HA Failover Inhibited

Alarm Type: PLAT

Description: Server HA Failover Inhibited -- This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.

Default Severity: Minor

OID: tpdHaInhibited

Recovery

Contact the Tekelec *Customer Care Center*.

32516 – Server HA Active To Standby Transition

Alarm Type: PLAT

Description: Server HA Active To Standby Transition -- This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Default Severity: Minor

OID: tpdHaActiveToStandbyTrans

Recovery

Contact the Tekelec *Customer Care Center*.

32517 – Server HA Standby To Active Transition

Alarm Type: PLAT

Description: Server HA Standby To Active Transition -- This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

Default Severity: Minor

OID: tpdHaStandbyToActiveTrans

Recovery

Contact the Tekelec *Customer Care Center*.

32518 – Platform Health Check Failure

Alarm Type: PLAT

Description: Platform Health Check Failure -- This alarm is used to indicate a configuration error.

Default Severity: Minor

OID: tpdHealthCheckFailed

Recovery

Contact the Tekelec *Customer Care Center*.

32519 – NTP Offset Check Failure

Alarm Type: PLAT

Description: NTP Offset Check Failure -- 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.

Default Severity: Minor

OID: ntpOffsetCheckFailed

Recovery

Contact the Tekelec *Customer Care Center*.

32520 – NTP Stratum Check Failure

Alarm Type: PLAT

Description: NTP Stratum Check Failure -- 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.

Default Severity: Minor

OID: ntpStratumCheckFailed

Recovery

Contact the Tekelec *Customer Care Center*.

32521 – SAS Presence Sensor Missing

Alarm Type: PLAT

Description: SAS Presence Sensor Missing -- This alarm indicates that the T1200 server drive sensor is not working.

Default Severity: Minor

OID: sasPresenceSensorMissing

Recovery

Contact the Tekelec *Customer Care Center* to get a replacement server.

32522 – SAS Drive Missing

Alarm Type: PLAT

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

Default Severity: Minor

OID: sasDriveMissing

Recovery

Contact the Tekelec *Customer Care Center* to determine whether the issue is with a failed drive or failed configuration.

32524 – HP disk resync

Alarm Type: PLAT

Description: HP disk resync -- 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 dependant on the size of the disk and the amount of activity on the system.

Default Severity: Minor

OID: tpdHpDiskResync

Recovery

Contact the Tekelec *Customer Care Center*.

32525 – Telco Fan Warning

Alarm Type: PLAT

Description: Telco Fan Warning -- This alarm indicates that the Telco switch has detected an issue with an internal fan.

Default Severity: Minor

OID: tpdTelcoFanWarning

Recovery

1. Contact the Tekelec *Customer Care Center* to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.
2. Tekelec *Customer Care Center* personnel can perform an snmpget command or log into the switch to get detailed fan status information.

32526 – Telco Temperature Warning

Alarm Type: PLAT

Description: Telco Temperature Warning -- This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.

Default Severity: Minor

OID: tpdTelcoTemperatureWarning

Recovery

1. Lower the ambient air temperature around the switch as low as possible.
2. If problem persists, contact the Tekelec *Customer Care Center*.

32527 – Telco Power Supply Warning

Alarm Type: PLAT

Description: Telco Power Supply Warning -- This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Default Severity: Minor

OID: tpdTelcoPowerSupplyWarning

Recovery

1. Verify breaker wasn't tripped.
2. If breaker is still good and problem persists, contact the Tekelec *Customer Care Center* who can perform a **snmpget** command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 – Invalid BIOS value

Alarm Type: PLAT

Description: Invalid BIOS value -- 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.

Default Severity: Minor

OID: tpdInvalidBiosValue

Recovery

Contact the Tekelec *Customer Care Center*.

32529 – Server Kernel Dump File Detected

Alarm Type: PLAT

Description: Server Kernel Dump File Detected -- This alarm indicates that the kernel has crashed and debug information is available.

Default Severity: Minor

OID: tpdServerKernelDumpFileDetected

Recovery

Contact the Tekelec *Customer Care Center*.

32530 – TPD Upgrade Fail Detected

Alarm Type: PLAT

Description: Server Upgrade Fail Detected -- This alarm indicates that a TPD upgrade has failed.

Default Severity: Minor

OID: tpdUpgradeFailed

Recovery

Contact the Tekelec *Customer Care Center*.

32531 – Half Open Socket Warning

Alarm Type: PLAT

Description: Half Open Socket Warning -- 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.

Default Severity: Minor

OID: tpdHalfOpenSocketWarning

Recovery

Contact the Tekelec *Customer Care Center*.

32532 – Server Upgrade Pending Accept/Reject

Alarm Type: PLAT

Description: Server Upgrade Pending Accept/Reject -- This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

Default Severity: Minor

OID: tpdServerUpgradePendingAccept

Recovery

Follow the steps in the application's upgrade procedure for accepting or rejecting the upgrade.

QBus Platform (70000-70999)

The QBus Platform (QP) software provides an execution environment for Java-based applications, which are the Multiprotocol Routing Agent (MRA), Multimedia Policy Engine (MPE), or the Configuration Management Platform (CMP). QP provides common interfaces into databases, event logging, SNMP, and cluster state. Two blades in the cluster provides 1+1 High-Availability (HA) protection. The application executes on one blade. The other blade acts as a hot standby in case the first blade fails to provide service.

70001 - QP_procmgr failed

Alarm Type: QP

Description: The QP-procmgr process has failed. This process manages all pcrf software.

Default Severity: Critical

Instance: N/A

HA Score: Failed

Clearing Action: This alarm is cleared by qp-procmgr after qp-procmgr is restarted.

OID: pcrfMIBNotificationsQPProcmgrFailedNotify

Recovery:

If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact the Tekelec *Customer Care Center*.

70002 - QP Critical process failed

Alarm Type: QP

Description: The QP-procmgr has detected that one of the critical processes it monitors has failed.

Default Severity: Critical

Instance: N/A

HA Score: Normal

Clearing Action: This alarm is cleared automatically.

OID:pcrfMIBNotificationsQPCriticalProcFailedNotify

Recovery:

This alarm automatically clears as Policy processes are restarted. If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact the Tekelec *Customer Care Center*.

70003 - QP Non-critical process failed

Alarm Type: QP

Description: The QP-procmgr has detected that one of the non-critical processes it monitors has failed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 60 seconds.

OID: pcrfMIBNotificationsQPNonCriticalProcFailedNotify

Recovery:

If the alarm occurs infrequently, monitor the health of the system. If the alarm occurs frequently, contact the Tekelec *Customer Care Center*.

70004 - QP Processes down for maintenance

Alarm Type: QP

Description: The QP processes have been brought down for maintenance.

Default Severity: Major

Instance: N/A

HA Score: Failed

Clearing Action: This alarm clears when the QP processes are restarted and exit maintenance.

OID: pcrfMIBNotificationsQPMaintShutdownNotify

Recovery:

If the alarm is occurring, confirm that the server is down for maintenance.

70010 - QP Failed Server-backup Remote Archive Rsync

Alarm Type: QP

Description: A scheduled backup failed to synchronize the local server-backup archive with the remote server-backup archive.

- Hostname=<hostname | IPaddr>
- path=<path>
- errorcode=<rsync error>

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 600 seconds (10 minutes).

OID: pcrfMIBNotificationsQPServerBackupRsyncFailedNotify

Recovery:

Check that the parameters are correct. Take corrective action based on the returned *Error Code Details for Alarms 70010 and 70011*.

Error Code Details for Alarms 70010 and 70011

Table 2: Error Code and Meaning - Alarms 70010/70011

Error Code	Meaning
1	Syntax or usage error
2	Protocol incompatibility
3	Errors selecting input/output files, dirs
4	Requested action not supported: an attempt was made to manipulate 64-bit files on a platform that cannot support them; or an option was specified that is supported by the client and not by the server

Error Code	Meaning
5	Error starting client-server protocol
6	Daemon unable to append to log-file
10	Error in socket I/O
11	Error in file I/O
12	Error in rsync protocol data stream
13	Errors with program diagnostics
14	Error in IPC code
20	Received SIGUSR1 or SIGINT
21	Some error returned by waitpid()
22	Error allocating core memory buffers
23	Partial transfer due to error
24	Partial transfer due to vanished source files
25	The --max-delete limit stopped deletions 30 Timeout in data send/receive
101	No mate found. Blade may be in degraded state
102	Called from master with '--fromMaster' option
103	Incorrect usage
104	Failed in key exchange with remote host

70011 - QP Failed System-backup Remote Archive Rsync

Alarm Type: QP

Description: A scheduled backup failed to synchronize the local system-backup archive with the remote system-backup archive.

Hostname=<hostname | IPaddr>, user=<user>, path=<path>,errorcode=<rsync error>

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 600 seconds.

OID: pcrfMIBNotificationsQPSystemBackupRsyncFailedNotify

Recovery:

Check that the parameters are correct. Take corrective action based on the returned *Error Code Details for Alarms 70010 and 70011*.

70012 - QP Failed To Create Server Backup

Alarm Type: QP

Description: A scheduled backup failed to create the local server-backup file.

Failure-reason=<errorcode>

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 600 seconds.

OID: pcrfMIBNotificationsQPServerBackupFailedNotify

Recovery:

Take corrective action based on the returned error message.

70013 - QP Failed To Create System Backup

Alarm Type: QP

Description: A scheduled backup failed to create the local system-backup file.

Failure-reason=<errorcode>

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 600 seconds.

OID: pcrfMIBNotificationsQPSystemBackupFailedNotify

Recovery:

Take corrective action based on the returned error message.

70015 - VIP Route Add Failed

Alarm Type: QP

Description: VIP Route Add Failed -- VIP route add failed to re-apply during VIP event.

The alarm displays the following information:

- IP-Type
- Route-Type
- Network
- Destination
- Gateway-Address
- Error Message

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 3600 seconds.

OID: pcrfMIBNotificationsQpAddRouteFailedNotify

Recovery:

Use server UI (Platcfg Routing Menu) to repair the route manually.

70020 - QP Master database is outdated

Alarm Type: QP

Description: The current MYSQL master server has an outdated database.

Default Severity: Critical

Instance: N/A

HA Score: Degraded

Clearing Action: This alarm clears when the master server either is made a slave server or if a database restore action clears the condition.

OID: pcrfMIBNotificationsQPMySQLMasterOutdatedNotify

Recovery:

1. Once the condition has occurred, the 80003 event will be sent once a minute. Wait until all of the expected servers are being reported. It is important to wait because the best slave might be undergoing a reboot and its DB Level will not be known until after the reboot completes.
2. Use the information in 80003 to select the new master candidate.
3. Except for the current master and the master candidate, put all of the other servers into forcedStandby.
4. If the best slave is in the same cluster (the most common case), simply perform a failover by restarting the current active blade. If the best slave is in a separate cluster, then a site promotion is necessary.
5. Remove the forced standby settings on the other slaves.
6. If none of the slaves are good candidates, perform a database restore.
   a) Put all of the slave servers into forced standby state
   b) Perform a restore on the active server.
      The restore will clear the condition.
   c) Take the slave servers out of the standby state.

70021 - QP slave database is unconnected to the master

Alarm Type: QP

Description: The MySQL slave is not connected to the master.

Default Severity: Major

Instance: N/A

HA Score: Failed

Clearing Action: This alarm clears automatically when the slave server connects to the master server.

OID:pcrfMIBNotificationsQPMySQLSlaveUnconnectedNotify

Recovery:

1. No action required unless the alarm does not clear within a few hours.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

70022 - QP Slave database failed to synchronize

Alarm Type: QP

Description: The MySQL slave failed to synchronize with the master.

Default Severity: Major

Instance: N/A

HA Score: Failed

Clearing Action: This alarm clears when the slave server synchronizes with the master server.

OID: pcrfMIBNotificationsQPMySQLSlaveSyncFailureNotify

Recovery:

1. No action required unless the alarm does not clear within a few hours.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

70023 - QP Slave database lagging the master

Alarm Type: QP

Description: The MySQL slave is lagging the master -- The MYSQL slave server is connected to the master server but its database has fallen behind the master database.

Default Severity: Minor

Instance: N/A

HA Score: Degraded

Clearing Action: This alarm clears automatically when the slave database is synchronized with the master database.

OID: pcrfMIBNotificationsQPMySQLSlaveLaggingNotify

Recovery:

1. No action required unless the alarm does not clear within a few hours or the condition is repeatedly set and unset.
2. If either of the problems persists, contact the Tekelec *Customer Care Center*.

70024 - QP Slave database is prevented from synchronizing with the master

Alarm Type: QP

Description: The MySQL slave has been prevented from sychronizing with the master -- The MySQL slave database has been prevented from synchronization with the master database because the master database is outdated.

Default Severity: Critical

Instance: N/A

HA Score: Degraded

Clearing Action: This alarm clears when the slave database is synchronized with the master database. This alarm is set on the slave server and will only occur when the active server on the primary site has set alarm 70020. This alarm clears automatically when the slave database is synchronized with the master database.

OID:pcrfMIBNotificationsQPMySQLSlaveSyncPreventedNotify

Recovery:

1. Diagnose the CMP master server to clear its 70020 alarm.
2. Once alarm 70020 is cleared, the slave server will clear alarm 70024.

70025 - QP Slave database is a different version than the master

Alarm Type: QP

Description: The MySQL slave has a different schema version than the master.

Default Severity: Critical

Instance: N/A

HA Score: Degraded

Clearing Action: The slave server clears the alarm when the master DB version is equal to the slave DB version.

OID:pcrfMIBNotificationsQPMySQLSchemaVersionMismatchNotify

Recovery:

This alarm is set by the CMP Slave Server during a CMP Server Upgrade or Backout, when the CMP Master Server DB is a different version than the CMP Slave Server DB. The Slave Server clears the alarm when the Master Server and the Slave Server again have the same version.

70026 - QP Server Symantec NetBackup Operation in Progress

Alarm Type: QP

Description: Server is performing a Symantec NetBackup Operation.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Alarm clears when the NetBackup client operation has completed.

OID: pcrfMIBNotificationsQPNetBackupInProgressNotify

Recovery:

1. When operation is complete, alarm should clear.
2. If the alarm does not clear within a few hours, then check the NetBackup Server logs.
3. If the NetBackup Server logs have no errors, or if the alarm is occurring over and over, contact Tekelec *Customer Care Center*.

Policy Server (71000-89999)

This section provides a list of Policy Server alarms (71000-79999) and events (80000-89999) which are generated by servers such as MPEs and MRAs.

71004 - AM CONN LOST

Alarm Type: PCRF

Description: AM socket closed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: AM connection restored to remote peer.

OID: pcrfMIBNotificationsAMConnLostNotify

Recovery:

1. Check the availability of the AM.
2. Check the AM log for a recent failover or other operations that can interrupt communications.
3. If the AM has not failed, make sure that the path from the AM to the MPE device (port 3918) is operational.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

71101 - DQOS DOWNSTREAM CONNECTION CLOSED

Alarm Type:PCRF

Description: DQoS Downstream connection is closed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: DQOS connection restored to a remote peer.

OID: pcrfMIBNotificationsDqosDownstreamConnectionClosedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

71102 - MSC CONN LOST

Alarm Type: PCRF

Description: MSC Conn Lost -- The connection was lost to the specified CMTS or downstream policy server.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to a remote peer is restored.

OID: pcrfMIBNotificationsMSCConnLostNotify

Recovery:

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (port 3918) is operational.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

71104 - DQOS AM CONNECTION CLOSED

Alarm Type: PCRF

Description: DQoS AM Connection Closed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to a remote peer is restored.

OID: pcrfMIBNotificationsDqosAmConnectionClosedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

71204 - SPC CONN CLOSED

Alarm Type: PCRF

Description: SPC SPC connection closed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to a remote peer is restored.

OID: pcrfMIBNotificationsSPCConnClosedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

71402 - TRANSPORT CLOSED

Alarm Type: PCRF

Description: Diameter Transport Closed -- A connection with a Diameter peer has been closed by a network element.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 7200 seconds.

OID: pcrfMIBNotificationsTransportClosedNotify

Recovery:

1. Check the configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the network element has not failed, ensure the network path from the device to the network element is operational.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

71403 - TRANSPORT DISCONNECTED

Alarm Type: PCRF

Description: Diameter Transport Disconnected -- Diameter connection socket is closed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 7200 seconds.

OID: pcrfMIBNotificationsTransportDisconnectedNotify

Recovery:

1. Check the configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.

3. If the network element has not failed, ensure the network path from the device to the network element is operational.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

71408 - DIAMETER NEW CONN REJECTED

Alarm Type: PCRF

Description: Diameter new connection rejected as an already functioning one exists. A Diameter peer (identified by its Diameter Identity) attempted to establish a connection with the device although it already has a valid connection. The Diameter protocol allows only one connection from a particular peer.

Note: This situation only occurs when DIAMETER.AllowMultipleConnectionsPerPeer is set to false, or when the multiple connections setting is turned off on the advanced tab of the policy server tab in the CMP GUI.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 300 seconds.

OID: pcrfMIBNotificationsDIAMETERNewConnRejectedNotify

Recovery:

1. Check the peer configuration and ensure that the peer sees a valid connection with the device.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

71414 - SCTP PATH STATUS CHANGED

Alarm Type: PCRF

Description: SCTP Path Status Changed -- Occurs when an MPE or MRA is multihoming. The alarm occurs when one path fails, and clears when the path becomes available again. If the path that is currently transmitting diameter messages fails, the alarm is triggered when the SCTP association tries to send the next diameter message. If the path is not transmitting diameter messages (it is a backup) then it may take up to 30 seconds for the alarm to be triggered, since heartbeat chunks are sent every 30 seconds.

Default Severity: Minor

Instance: Peer address + Association ID

HA Score: Normal

Clearing Action: This alarm clears automatically after 7200 seconds.

OID: pcrfMIBNotificationsSctpPathStatusChangedNotify

Recovery:

If the problem persists, contact the Tekelec *Customer Care Center*.

71605 - LDAP CONN FAILED

Alarm Type: PCRF

Description: Connection to LDAP server failed.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to LDAP server is restored.

OID: pcrfMIBNotificationsLdapConnFailedNotify

Recovery:

Verify that there is no problem with the LDAP server or the network path used to reach the server. If the problem persists, contact the Tekelec *Customer Care Center*.

71630 - DHCP UNEXPECTED EVENT ID

Alarm Type: PCRF

Description: DHCP Communication exception.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Next successful DHCP operation will clear this alarm.

OID: pcrfMIBNotificationsDHCPUnexpectedEventIdNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

71631 - DHCP UNABLE TO BIND EVENT ID

Alarm Type: PCRF

Description: DHCP unable to bind event ID.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Next successful DHCP bind operation will clear this alarm.

OID: pcrfMIBNotificationsDHCPUnableToBindEventIdNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

71632 - DHCP RESPONSE TIMEOUT EVENT ID

Alarm Type: PCRF

Description: DHCP Response Timeout Event Id.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 60 seconds.

OID: pcrfMIBNotificationsDHCPResponseTimeoutEventIdNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

71633 - BAD RELAY ADDRESS EVENT ID

Alarm Type: PCRF

Description: DHCP bad relay address event id.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 30 seconds.

OID: pcrfMIBNotificationsDHCPBadRelayAddressEventIdNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

71634 - DHCP BAD PRIMARY ADDRESS EVENT ID

Alarm Type: PCRF

Description: DHCP no primary address specified.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 30 seconds.

OID: pcrfMIBNotificationsDHCPBadPrimaryAddressEventIdNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

71635 - DHCP BAD SECONDARY ADDRESS_EVENT ID

Alarm Type: PCRF

Description: DHCP no secondary address specified.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 30 seconds.

OID: pcrfMIBNotificationsDHCPBadSecondaryAddressEventIdNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

71684 - SPR CONNECTION CLOSED

Alarm Type: PCRF

Description: SPR Closing a secondary connection to revert to primary connection.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to SPR is restored.

OID: pcrfMIBNotificationsSPRConnectionClosedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

71685 - MSR DB NOT REACHABLE

Alarm Type: PCRF

Description: Unable to connect to MSR after several attempts.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to MSR is restored.

OID: pcrfMIBNotificationsMSRDBNotReachableNotify

Recovery:

Verify that there is no problem with the MSR server or the network path used to reach the server. If the problem persists, contact the Tekelec *Customer Care Center*.

71702 - BRAS CONNECTION CLOSED

Alarm Type: PCRF

Description: Bras Connection Closed -- The MPE lost a connection to the B-RAS element of the gateway.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to BRAS is restored.

OID: pcrfMIBNotificationsBrasConnectionClosedNotify

Recovery:

1. Check availability of the gateway.
2. If the gateway has not failed, make sure that the path from the gateway to the MPE is operational.
3. If the problem persists, contact the Tekelec *Customer Care Center*.

71703 - COPS UNKNOWN GATEWAY

Alarm Type: PCRF

Description: COPS Unknown Gateway -- An unknown gateway is trying to establish a COPS-PR connection to the MPE.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: COPS network element is associated with MPE.

OID: pcrfMIBNotificationsCOPSUnknownGatewayNotify

Recovery:

1. Check the configuration of the network elements in the CMP. There should be a B-RAS network element for this gateway and that B-RAS must be associated with this MPE.
   Make sure that the configuration of the B-RAS network element is consistent with the provisioned information on the gateway. The network element name in the CMP must match the provisioned router name on the gateway.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

71801 - PCMM NO PCEF

Alarm Type: PCRF

Description: PCMM no PCEF.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 60 seconds.

OID: pcrfMIBNotificationsPCMMNoPCEFNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

71805 - PCMM NOCONNECTION PCEF

Alarm Type: PCRF

Description: PCMM Non Connection to PCEF.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 60 seconds.

OID: pcrfMIBNotificationsPCMMNonConnectionPCEFNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

72198 - SMSR SMSC SWITCHED TO PRIMARY

Alarm Type: SMS

Description: Switched to primary SMSC -- Switched from Secondary to Primary SMSC.

Default Severity: Minor

Instance: SMSC address

HA Score: Normal

Clearing Action: Auto clear after 60 minutes

OID: pcrfMIBNotificationsSMSRSMTPConnectionClosedNotify

Recovery:

No action necessary.

72199 - SMSR SMSC SWITCHED TO SECONDARY

Alarm Type: SMPP

Description: Switched to Secondary SMSC -- Switched from Primary to Secondary SMSC.

Default Severity: Minor

Instance: SMSC Address

HA Score: Normal

Clearing Action: Auto clear after 60 minutes

OID: pcrfMIBNotificationsSMSRSMTPConnectionClosedNotify

Recovery:

No action necessary.

72210 - PCMM REACHED MAX GATES EVENT ID

Alarm Type: PCRF

Description: PCMM Reached Maximum Gates -- A subscriber at IP address ip-addr has reached the configured maximum number of upstream gates.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 60 seconds.

OID: pcrfMIBNotificationsPCMMReachedMaxGatesEventIdNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

72211 - PCMM REACHED MAX GPI EVENT ID

Alarm Type: PCRF

Description: PCMM Reached Maximum GPI -- PCMM reached maximum GPI. A subscriber at IP address ip-addr has reached the configured maximum grants per interval on all upstream gates.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears automatically after 60 seconds.

OID: pcrfMIBNotificationsPCMMReachedMaxGPIEventIdNotify

Recovery:

1. This subscriber address is exceeding the capacity; attention is required.
2. Contact the Tekelec *Customer Care Center*.

72501 - SCE CONNECTION LOST

Alarm Type: PCRF

Description: SCE Connection is lost.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Connection to SCE is restored.

OID: pcrfMIBNotificationsSCEConnectionLostNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

72549 - SMSR QUEUE FULL

Alarm Type: PCRF

Description: SMSR queue full -- SMSR internal queue has reached capacity. This will result in messages being dropped until the queue is free to accept new messages.

Default Severity: Minor

Instance: SMSR queue

HA Score: Normal

Clearing Action: Auto clear after 60 minutes

OID: pcrfMIBNotificationsSMSRSMTPConnectionClosedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

72559 - SMSR SMSC CONN CLOSED

Alarm Type: PCRF

Description: SMSC connection closed.

Default Severity: Minor

Instance: SMSC address

HA Score: Normal

Clearing Action: Auto clear after 60 minutes

OID: SMSRSMTPConnectionClosed

Recovery:

No action necessary.

72565 - SMSR SMTP CONN CLOSED

Alarm Type: PCRF

Description: SMTP connection closed -- SMTP connection has been closed to MTA {IP Address}.

Default Severity: Minor

Instance: {hostname of MTA}

HA Score: Normal

Clearing Action: Auto clear after 60 minutes

OID: pcrfMIBNotificationsSMSRSMTPConnectionClosedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

72703 - RADIUS SERVER START FAILED

Alarm Type: PCRF

Description: RADIUS server start failed.

Default Severity: Minor

Instance: N/A

HA Score: N/A

Clearing Action: TBD

OID: pcrfMIBNotificationsRADIUSServerFailedNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

72706 - RADIUS SERVER CORRUPT AUTH

Alarm Type: PCRF

Description: RADIUS authenticator is corrupted.

Default Severity: Minor

Instance: N/A

HA Score: N/A

Clearing Action: TBD

OID: pcrfMIBNotificationsRADIUServerCorrupAuthNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

72904 - DIAMETER TOO BUSY

Alarm Type: PCRF

Description: Diameter load shedding set a busy state.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: The Diameter load drops below admission criteria thresholds or this alarm clears automatically after 30 seconds.

OID: pcrfMIBNotificationsDiameterTooBusyNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

72905 - RADIUS TOO BUSY

Alarm Type: PCRF

Description: RADIUS load shedding set a busy state.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: The RADIUS load drops below admission criteria thresholds or this alarm clears automatically after 30 seconds.

OID: pcrfMIBNotificationsRadiusTooBusyNotify

Recovery:

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact the Tekelec *Customer Care Center*.

74000 - POLICY CRITICAL ALARM

Alarm Type: PCRF

Description: Critical Policy alarm.

Default Severity: Critical

Instance: N/A

HA Score: Normal

Clearing Action: This alarm can be cleared by a policy or clears automatically after 3600 seconds (one hour).

OID: pcrfMIBNotificationsPolicyServerCriticalAlarmNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

74001 - POLICY MAJOR ALARM

Alarm Type: PCRF

Description: Major Policy alarm.

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm can be cleared by a policy or clears automatically after 3600 seconds (one hour).

OID: pcrfMIBNotificationsPolicyServerMajorAlarmNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

74002 - POLICY MINOR ALARM

Alarm Type: PCRF

Description: Minor Policy alarm.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm can be cleared by a policy or clears automatically after 3600 seconds (one hour).

OID: pcrfMIBNotificationsPolicyServerMajorAlarmNotify

Recovery:

Contact the Tekelec *Customer Care Center*.

74020 - DELETE EXPIRE FILES

Alarm Type: PCRF

Description: Delete expire files -- Stats Files Generator Task has removed some files which weren't synced to remote servers (<external system IP>,<external system IP>, etc).

Default Severity: Major

Instance: Stats files generator

HA Score: Normal

Clearing Action: Auto clear 300 seconds

OID: pcrfMIBNotificationsFilesGeneratorDeleteExpireFilesNotify

Recovery:

Check all enabled Stats Files Synchronization tasks status in the DC (Data Collection) tasks of CMP, and ensure they are configured successfully.

74021 - FILE SYNCHRONIZATION FAILURE

Alarm Type: PCRF

Description: Files synchronization failure -- Stats Files Synchronization #<X> task failed to sync local to remote server (<external system Host Name/IP>) after retry <N> times, where:

- X: task #
- N: 1-5 retry times
- External system Host Name/IP: user-defined remote server's address to which files are synced

Default Severity: Minor

Instance: Stats files synchronization

HA Score: Normal

Clearing Action: Auto clear 300 seconds

OID: pcrfMIBNotificationsFilesSynchronizationFailureNotify

Recovery:

Check the network status of the remote server which you configured in the Stats Files Synchronization task; ensure remote server supports SSH protocol and you configured the user name and password correctly.

74602 - QP Multiple Active In Cluster Failure

Alarm Type: QP

Description: Multiple Active servers have been detected in the same cluster; the cluster is in Split Brain state.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears when HA recovers or can clears automatically after 30 minutes. When HA recovers there will be only one Active server in a cluster.

OID: pcrfMIBNotificationsQPMultipleActiveInClusterFailureNotify

Recovery:

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. Contact the Tekelec *Customer Care Center*.

74603 - QP Max Primary Cluster Failure Threshold

Alarm Type: QP

Description: The number of failed MPE pairs reaches the threshold of {Max Primary Site Failure Threshold} at {Site}, where:

- Max Primary Site Failure Threshold is the configured threshold value
- Site is the site name

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears when the number of failed MPE pairs remain at a lower value than the threshold of {Max Primary Site Failure Threshold} at {Site}, or clears automatically after 30 minutes.

OID: pcrfMIBNotificationsQPMaxMPEPrimaryClusterFailureNotify

Recovery:

1. When the failure count drops below the threshold value and stays below the threshold for 30 seconds, the alarm is cleared. (The 30 seconds delay prevents the alarm from being cleared too soon.)
2. If alarm doesn't clear automatically, contact the Tekelec *Customer Care Center*.

74604 - QP Policy Cluster Offline Failure

Alarm Type: QP

Description: Policy Cluster is offline.

Default Severity: Critical

Instance: N/A

HA Score: Normal

Clearing Action: This alarm clears when a server in the MPE cluster comes online. The alarm clears automatically after 30 minutes.

OID: pcrfMIBNotificationsQPMPEClusterOfflineFailureNotify

Recovery:

1. When a server comes online (in Active, Standby, or Spare state), the alarm is cleared. Please check whether all servers are powered down or rebooted at that time.
2. If alarm doesn't clear automatically, contact the Tekelec *Customer Care Center*.

75000 - POLICY LIBRARY LOADING FAILED

Alarm Type: PCRF

Description: Policy library loading failed -- PCRF was unable to load the latest policy library. If this alarm occurred at startup time or at failover, this indicates the PCRF does not have any policies deployed. If this alarm occurred on a new policy push when PCRF was running with some existing policies, this alarm indicates that the PCRF will continue to run with those existing policies.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Performing a reapply config may fix the problem.

OID: pcrfMIBNotificationsPolicyLoadingLibraryFailedNotify

Recovery:

1. Perform a reapply config from the CMP to reload the library.
2. If the problem persists, contact the Tekelec *Customer Care Center*.

78000 - ADS CONNECTION LOST

Alarm Type: PCRF

Description: ADS Connection Lost -- The Analytics Data Stream (ADS) connection was lost to the specified client.

Default Severity: Minor

Instance: Analytics Client ID

HA Score: Normal

Clearing Action: Connection to a remote peer is restored by the same client (ID), or in one hour by auto clear.

OID: pcrfMIBNotificationsADSConnectionLostNotify

Recovery:

1. Check configuration and availability of the analytics client.
2. Check the client for reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (port 222) is operational.
4. If the problem persists, contact the Tekelec *Customer Care Center*.

78001 - RSYNC FAILED

Alarm Type: PCRF

Description: Transfer of Policy jar files failed -- PCRF was unable to transfer the latest policy library from the active to the standby server. The alarm can be raised by the active when a policy change is

made or a Reapply Configuration is performed. It can be raised by the standby during startup if it was unable to get the policy jar file from the active during startup.

Default Severity: Minor

Instance: N/A

HA Score: Normal

Clearing Action: Since the alarm can be raised by both the active and standby servers, the alarm will not clear once the problem is fixed; it will auto-clear in an hour.

OID: pcrfMIBNotificationsRsyncFailedNotify

Recovery:

1. This alarm can be ignored during a mixed version upgrade (eg. 7.5/7.6 -> 9.1) and when rebooting both servers on the MPE.
2. If the alarm is seen on the MRA, it indicates the logback config files are not transferring, which is harmless to the operation.
3. The most likely cause is that the ssh keys have not been exchanged; ensure they are exchanged correctly.
4. Perform a Reapply Configuration.
5. If performing a Reapply Configuration does not fix the problem, another alarm will be raised by the active server for that particular operation. If the problem persists, contact the Tekelec *Customer Care Center*.
6. The original alarm will auto-clear in an hour.

80001 - QP DB State Transition

Alarm Type: QP

Description: The DB status of the blade is not fully ready -- The MySQL database manager generates a "MySQL state transition" event every time it makes a state-machine transition. The event text describes the transition.

Default Severity: Info

Instance: MySQL

HA Score: Normal

Clearing Action: This alarm is cleared by qp-procmgr as qp-procmgr shuts down.

OID: pcrfMIBNotificationsQPDBStateChangeNotify

Recovery:

No action required.

80002 - QP MySQL Relay Log Dropped

Alarm Type: QP

Description: A portion of the MySQL relay log was dropped as the slave was shutting down -- This event is raised when a slave server times out while trying to apply its relay log during a slave stop.

The server may not be hurt, but there may be aftereffects. This event is raised to trigger a debug for possible aftereffects.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsQPMySQLRelayLogDroppedNotify

Recovery:

Debug the system for possible aftereffects caused by the timeout.

80003 - QP MySQL Database Level Advertisement

Alarm Type: QP

Description: The ranking of slaves when the master is outdated -- If the master database is outdated, the server raises this event once per minute. The server will rank the slaves, from best to worst, based on their database level .

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsQPMySQLDBLevelNotify

Recovery:

Use the information of this event to help resolve an outdated master database raised by alarm 70020.

82704 - BINDING RELEASE TASK

Alarm Type: PCRF

Description: Binding Release Task -- The binding release task has started, completed, or aborted.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsBindingReleaseTaskNotify

Recovery:

No action required.

84004 - POLICY INFO EVENT

Alarm Type: PCRF

Description: Policy Info Event -- Application is ready.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsPolicyInfoEventNotify

Recovery:

No action required.

86001 - APPLICATION IS READY

Alarm Type: PCRF

Description: Application is ready for service.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsApplicationIsReadyNotify

Recovery:

No action required.

86100 - CMP USER LOGIN

Alarm Type: PCRF

Description: CMP User login -- User [ABC] login succeeded.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsCMPUserLoginNotify

Recovery:

No action required.

86101 - CMP USER LOGIN FAILED

Alarm Type: PCRF

Description: CMP User login failed -- User [ABC] login failed.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsCMPUserLoginFailedNotify

Recovery:

No action required.

86102 - CMP USER LOGOUT

Alarm Type: PCRF

Description: CMP User logout -- User [ABC] logout.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsCMPUserLogoutNotify

Recovery:

No action required.

86200 - CMP USER PROMOTED SERVER

Alarm Type: PCRF

Description: CMP User promoted server -- Application is ready.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsCMPUserPromotedServerNotify

Recovery:

No action required.

86201 - CMP USER DEMOTED SERVER

Alarm Type: PCRF

Description: CMP User demoted server -- User [ABC] demoted [1/2] CMP.

Default Severity: Info

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID:pcrfMIBNotificationsCMPUserDemotedServerNotify

Recovery:

No action required.

86300 - SH ENABLE FAILED

Alarm Type: PCRF

Description: Enable Sh Connection failed -- The CMP performed a global operation to enable Sh on all MPE's and it failed on the specified MPE.

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsCMPShConEnableFailedNotify

Recovery:

The operation can be retried. If repeated attempts fail then there may be other management issues with the associated MPEs and connectivity to those devices should be verified.

86301 - SH DISABLE FAILED

Alarm Type: PCRF

Description: Disable Sh Connection failed -- The CMP performed a global operation to disable Sh on all MPE's and it failed on the specified MPE.

Default Severity: Major

Instance: N/A

HA Score: Normal

Clearing Action: N/A

OID: pcrfMIBNotificationsCMPShConDisableFailedNotify

Recovery:

The operation can be retried. If repeated attempts fail then there may be other management issues with the associated MPEs and connectivity to those devices should be verified.

Glossary

A

AM	application manager A server within a network that is responsible for establishing and managing subscriber sessions associated with a specific application.
AMID	Application Manager ID

B

B-RAS	broadband remote access server

C

CMP	Configuration Management Platform A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.
CMTS	Cable modem termination system An edge device connecting to subscribers' cable modems in a broadband network. A CMTS device can function as a PCEF device; see PCEF.

D

DC	Data Collection
DNS	Domain Name System A system for converting Internet host and domain names into IP addresses.

D

DQoS	Dynamic Quality of Service A COPS-based protocol that is part of the Packet Cable standards used to communicate between a CMS and a CMTS for setting up voice calls. An MPE device can be inserted between these two entities to apply additional policy rules as sessions are established.

G

GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

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.
HP	Hewlett-Packard
HSS	Home Subscriber Server A central database for subscriber information.

L

LDAP	Lightweight Directory Access Protocol A protocol for providing and receiving directory information in a TCP/IP network.

M

M

MPE	Multimedia Policy Engine A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a protocol-independent policy rules engine that provides authorization for services based on policy conditions such as subscriber information, application information, time of day, and edge resource utilization.
MRA	Multi-Protocol Routing Agent Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices.
MSR	Multimedia Subscriber Repository
MTA	Major Trading Area
Multimedia Policy Engine	See MPE.
Multiprotocol Routing Agent	See MRA.

N

NTP	Network Time Protocol

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

O

	organizations. Vendors define private branches that include managed objects for their own products.
OSS	Operations Support System Computer systems used by telecommunications service providers, supporting processes such as maintaining network inventory, provisioning services, configuring network components, and managing faults.
OSSI	Operation Support System Interface An interface to a "back-end" (office) system. The Configuration Management Platform includes an OSSI XML interface.

P

PCEF	Policy and Charging Enforcement Function Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.
PCMM	PacketCable MultiMedia
PCRF	Policy and Charging Rules Function The ability to dynamically control access, services, network capacity, and charges in a network.

Q

Q

QBus Platform	See QP.
QP	QBus Platform Software that provides an execution environment for Java-based applications, providing common interfaces into databases, event logging, SNMP, and cluster state.

R

RKS	Record Keeping Server

S

SCTP	Stream Control Transmission Protocol SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SMPP	Short Message Peer-to-Peer Protocol An open, industry standard protocol that provides a flexible data communications interface for transfer of short message data.
SMSR	SMS Relay Application An interface between the MPE and SMSC or other specific SMS web service(s).
SMTP	Simple Mail Transfer Protocol

S

SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAP	Simple Object Access Protocol
SPC	Service Provisioning over COPS (Common Open Policy Service protocol)