

**Oracle® Communications
Policy Management**

SNMP User's Guide

Release 9.7.4

E70980 Revision 01

April 2016

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

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

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

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

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

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

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

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

Table of Contents

Chapter 1: About This Guide.....	14
How This Guide is Organized.....	15
Scope and Audience.....	15
Documentation Admonishments.....	15
Related Publications.....	16
Locate Product Documentation on the Oracle Help Center Site.....	16
Customer Training.....	16
My Oracle Support (MOS).....	17
Emergency Response.....	17
 Chapter 2: Overview.....	 18
Simple Network Management Protocol.....	19
The SNMP Standard.....	19
SNMP Message Types.....	19
Standard Managed Objects.....	20
 Chapter 3: Configuring SNMP.....	 21
About SNMP Configuration.....	22
SNMP Versions.....	23
Configuring SNMP Settings.....	23
 Chapter 4: Supported MIBs.....	 26
Supported MIBs.....	27
SNMP MIB Objects.....	27
MIB Object Access Values.....	28
Compiling MIB Objects.....	28
 Chapter 5: Support for Traps.....	 30
Alarms Overview.....	31
Alarms formatting information.....	32
Alarm and Event Severity Levels.....	34

Platform (31000-32800).....	34
31000- S/W fault.....	34
31001 - S/W status.....	35
31002 - Process watchdog failure.....	35
31003 - Tab thread watchdog failure.....	35
31100 - Database replication fault.....	36
31101 - Database replication to slave failure.....	36
31102 - Database replication from master failure.....	37
31103 - DB Replication update fault.....	37
31104 - DB Replication latency over threshold.....	37
31105 - Database merge fault.....	38
31106 - Database merge to parent failure.....	38
31107 - Database merge from child failure.....	38
31108 - Database merge latency over threshold.....	39
31109 - Topology config error.....	39
31110 - Database audit fault.....	40
31111 - Database merge audit in progress.....	40
31112 - DB replication update log transfer timed out.....	40
31113 - DB replication manually disabled.....	41
31114 - DB replication over SOAP has failed.....	41
31115 - Database service fault.....	41
31116 - Excessive shared memory.....	42
31117 - Low disk free.....	42
31118 - Database disk store fault.....	43
31119 - Database updatelog overrun.....	43
31120 - Database updatelog write fault.....	43
31121 - Low disk free early warning.....	44
31122 - Excessive shared memory early warning.....	44
31123 - Database replication audit command complete.....	44
31124 - ADIC error.....	45
31125 - Database durability degraded.....	45
31126 - Audit blocked.....	46
31127 - DB Replication Audit Complete.....	46
31128 - ADIC Found Error.....	46
31129 - ADIC Found Minor Issue.....	47
31130 - Network health warning.....	47
31131 - DB Ousted Throttle Behind.....	47
31140 - Database perl fault.....	48
31145 - Database SQL fault.....	48
31146 - DB mastership fault.....	48
31147 - DB upsynclog overrun.....	49

31148 - DB lock error detected.....	49
31200 - Process management fault.....	50
31201 - Process not running.....	50
31202 - Unkillable zombie process.....	50
31206 - Process mgmt monitoring fault.....	51
31207 - Process resource monitoring fault.....	51
31208 - IP port server fault.....	51
31209 - Hostname lookup failed.....	52
31213 - Process scheduler fault.....	52
31214 - Scheduled process fault.....	53
31215 - Process resources exceeded.....	53
31216 - SysMetric configuration error.....	53
31220 - HA configuration monitor fault.....	54
31221 - HA alarm monitor fault.....	54
31222 - HA not configured.....	54
31223 - HA Heartbeat transmit failure.....	55
31224 - HA configuration error.....	55
31225 - HA service start failure.....	55
31226 - HA availability status degraded.....	56
31227 - HA availability status failed.....	56
31228 - HA standby offline.....	57
31229 - HA score changed.....	57
31230 - Recent alarm processing fault.....	57
31231 - Platform alarm agent fault.....	58
31232 - Late heartbeat warning.....	58
31233 - HA Path Down.....	58
31234 - Untrusted Time Upon Initialization	59
31235 - Untrusted Time After Initialization	59
31236 - HA Link Down.....	60
31240 - Measurements collection fault.....	60
31250 - RE port mapping fault.....	61
31260 - SNMP Agent.....	61
31270 - Logging output.....	61
31280 - HA Active to Standby transition.....	62
31281 - HA Standby to Active transition.....	62
31282 - HA Management Fault.....	62
31283 - Lost Communication with server.....	63
31284 - HA Remote Subscriber Heartbeat Warning.....	63
31285 - HA Node Join Recovery Entry.....	64
31286 - HA Node Join Recovery Plan.....	64
31287 - HA Node Join Recovery Complete.....	64

31290 - HA Process Status.....	65
31291 - HA Election Status.....	65
31292 - HA Policy Status.....	65
31293 - HA Resource Link Status.....	66
31294 - HA Resource Status.....	66
31295 - HA Action Status.....	67
31296 - HA Monitor Status.....	67
31297 - HA Resource Agent Info.....	67
31298 - HA Resource Agent Detail.....	68
31299 - HA Notification Status.....	68
31300 - HA Control Status.....	68
31301 - HA Topology Events.....	69
32113 - Uncorrectable ECC memory error.....	69
32114 - SNMP get failure.....	70
32115 - TPD NTP Daemon Not Synchronized Failure.....	70
32116 - TPD Server's Time Has Gone Backwards.....	70
32117 - TPD NTP Offset Check Failure.....	71
32300 - Server fan failure.....	71
32301 - Server internal disk error.....	72
32303 - Server Platform error.....	72
32304 - Server file system error.....	72
32305 - Server Platform process error.....	73
32307 - Server swap space shortage failure.....	73
32308 - Server provisioning network error.....	74
32312 - Server disk space shortage error.....	74
32313 - Server default route network error.....	75
32314 - Server temperature error.....	75
32315 - Server mainboard voltage error.....	76
32316 - Server power feed error.....	76
32317 - Server disk health test error.....	77
32318 - Server disk unavailable error.....	78
32320 - Device interface error.....	78
32321 - Correctable ECC memory error.....	78
32322 - Power Supply A error.....	79
32323 - Power Supply B error.....	79
32324 - Breaker panel feed error.....	80
32325 - Breaker panel breaker error.....	80
32326 - Breaker panel monitoring error.....	82
32327 - Server HA Keepalive error.....	83
32331 - HP disk problem.....	84
32332 - HP Smart Array controller problem.....	84

32333 - HP hpacucliStatus utility problem.....	84
32335 - Switch link down error.....	85
32336 - Half Open Socket Limit.....	85
32337 - Flash Program Failure.....	86
32338 - Serial Mezzanine Unseated.....	86
32339 - Max pid limit.....	87
32340 - Server NTP Daemon Lost Synchronization For Extended Time.....	87
32341 - Server NTP Daemon Never Synchronized Error.....	87
32342 - NTP Offset Check Error.....	88
32343 - RAID disk problem.....	88
32344 - RAID controller problem.....	89
32345 - Server Upgrade snapshot(s) invalid.....	89
32346 - Server Hardware Problem.....	89
32347 - Oracle hwmgmtcliStatus Problem.....	90
32348 - FIPS subsystem problem.....	90
32349 - File Tampering.....	91
32350 - Security Process Terminated.....	91
32500 - Server disk space shortage warning.....	91
32501 - Server application process error.....	92
32502 - Server hardware configuration error.....	92
32505 - Server swap space shortage warning.....	93
32506 - Server default router not defined.....	93
32507 - Server temperature warning.....	94
32508 - Server core file detected.....	94
32509 - Server NTP Daemon not synchronized.....	95
32510 - CMOS battery voltage low.....	95
32511 - Server disk self test warning.....	96
32512 - Device warning.....	96
32513 - Device interface warning.....	97
32514 - Server reboot watchdog initiated.....	97
32515 - Server HA failover inhibited.....	98
32516 - Server HA Active to Standby transition.....	98
32517 - Server HA Standby to Active transition.....	98
32518 - Platform Health Check failure.....	99
32519 - NTP Offset Check failure.....	99
32520 - NTP Stratum Check failure.....	100
32521 - SAS Presence Sensor Missing.....	100
32522 - SAS Drive Missing.....	100
32524 - HP disk resync.....	101
32525 - Telco Fan Warning.....	101
32526 - Telco Temperature Warning.....	102

32527 - Telco Power Supply Warning.....	102
32528 - Invalid BIOS value.....	103
32529 - Server Kernel Dump File Detected.....	103
32530 - Server Upgrade Fail Detected.....	104
32531 - Half Open Socket Warning.....	104
32532 - Server Upgrade Pending Accept/Reject.....	104
32533 - Max pid warning.....	105
32534 - NTP Source Server Is Not Able To Provide Correct Time.....	105
32535 - RAID disk resync.....	106
32536 - Server Upgrade snapshot(s) warning.....	106
32540 - Power limit mismatch.....	107
32700 - Telco Switch Notification.....	107
32701 - HIDS Initialized.....	107
32702 - HIDS Baseline Deleted.....	108
32703 - HIDS Enabled.....	108
32704 - HIDS Disabled.....	108
32705 - HIDS Monitoring Suspended.....	108
32706 - HIDS Monitoring Resumed.....	109
32707 - HIDS Baseline Updated.....	109
QBus Platform (70000-70999).....	109
70001 – QP_procmgr failed.....	109
70002 – QP Critical process failed.....	110
70003 – QP Non-critical process failed.....	110
70004 – QP Processes down for maintenance.....	110
70005 – QP Cluster Status.....	111
70006 - QP Blade Status.....	111
70008 - QP Database Service Failed.....	112
70009 – QP Topology Configuration Mismatch.....	112
70010 – QP Failed Server-backup Remote Archive Rsync.....	113
70011 – QP Failed System-backup Remote Archive Rsync.....	113
70012 – QP Failed To Create Server Backup.....	113
70013 – QP Failed To Create System Backup.....	114
70015 – Route Add Failed.....	114
70016 – No Available VIP Route	115
70017 – No Available Static IP.....	115
70020 – QP Master database is outdated.....	116
70021 – QP slave database is unconnected to the master.....	116
70022 – QP Slave database failed to synchronize.....	117
70023 – QP Slave database lagging the master.....	117
70024 - QP Slave database is prevented from synchronizing with the master.....	117
70025 – QP Slave database is a different version than the master.....	118

70026 – QP Server Symantec NetBackup Operation in Progress.....	118
70028 – QP bonded interface is down.....	119
70029 – QP peer node bonded interface is down.....	119
70030 – QP backplane bonded interface is down.....	119
70031 – QP degrade because one or more interfaces are down.....	120
70032 – QP direct link does not work as configuration.....	120
70038 – QP has blocked IPv4 traffic on an OAM interface.....	121
70039 – QP has blocked IPv4 traffic on all interfaces.....	121
70040 – Failure to block IPv4 on the OAM interface.....	121
70041 – Failure to block IPv4 on the all interfaces.....	122
70042 – Failure to remove OAM IPv4 addresses from the cluster/site.....	122
70043 – Failure to remove all IPv4 addresses from the cluster/site.....	123
70044 – Failure to rollback changes for removing IPv4 addresses.....	123
70050 – QP Timezone change detected.....	123
70500 – System Mixed Version.....	124
70501 – Cluster Mixed Version.....	124
70502 – Cluster Replication Inhibited.....	125
70503 – Server Forced Standby.....	125
70505 – ISO Mismatch.....	126
70506 – Upgrade Operation Failed.....	126
70507 – Upgrade In Progress.....	126
70508 – Server Is Zombie.....	127
Policy Server Alarms (71000-79999).....	127
71001 – Remote Diversion Not Possible.....	127
71002 – OM Stats Parse Error.....	128
71003 – OM Stats Exception Error.....	128
71004 – AM Conn Lost.....	128
71005 – OM Stats Value Exceed Error.....	129
71101 – DQOS Downstream Connection Closed.....	129
71102 – MSC Conn Lost.....	129
71103 – PCMM Conn Lost.....	130
71104 – DQOS AM Connection Closed.....	130
71204 – SPC Conn Closed.....	131
71402 – Connectivity Lost.....	131
71403 – Connectivity Degraded.....	131
71408 – Diameter New Conn Rejected.....	132
71414 – SCTP Path Status Changed.....	132
71605 – LDAP Conn Failed.....	133
71630 – DHCP Unexpected Event ID.....	133
71631 – DHCP Unable to Bind Event ID.....	134
71632 – DHCP Response Timeout Event ID.....	134

71633 – DHCP Bad Relay Address Event ID.....	134
71634 – DHCP Bad Primary Address Event ID.....	135
71635 – DHCP Bad Secondary Address Event ID.....	135
71684 – SPR Connection Closed.....	135
71685 – MSR DB Not Reachable.....	136
71702 – BRAS Connection Closed.....	136
71703 – COPS Unknown Gateway.....	136
71801 – PCMM No PCEF.....	137
71805 – PCMM Non Connection PCEF.....	137
72198 – SMSR SMSC Switched to Primary.....	138
72199 – SMSR SMSC Switched to Secondary.....	138
72210 – PCMM Reached Max Gates Event ID.....	138
72211 – PCMM Reached Max GPI Event ID.....	139
72501 – SCE Connection Lost.....	139
72549 – SMSR Queue Full.....	140
72559 – SMSR SMSC Connection Closed.....	140
72565 – SMSR SMTP Connection Closed.....	140
72575 – SMSR HTTP Connection Closed.....	141
72703 – RADIUS Server Failed.....	141
72706 – RADIUS Server Corrupt Auth.....	142
72904 – Diameter Too Busy.....	142
72905 – Radius Too Busy.....	142
74000 – Policy Server Critical Alarm.....	143
74001 – Policy Server Major Alarm.....	143
74002 – Policy Server Minor Alarm.....	143
74020 – Stats Files Generator Delete Expire Files.....	144
74021 – Files Synchronization Failure.....	144
74022 – Files Uploading Failure.....	145
74102 – CMTS Subnet Overlapped.....	145
74103 – NES Without CMTS IP.....	145
74602 – Multiple Active In Cluster Failure.....	146
74603 – Max Primary Cluster Failure Threshold.....	146
74604 – MPE Cluster Offline Failure.....	147
74605 – Subscriber Trace Backup Failure.....	147
75000 – Policy Library Loading Failed.....	147
77904 – BOD PCMM Too Busy.....	148
77905 – BOD DIAMETER Too Busy.....	148
78000 – ADS Connection Lost.....	149
78001 – Rsync Failed.....	149
79002 – Sess DB Size Reached Threshold	150
79003 – Avg Sess Size Reached Threshold.....	150

79004 - Bind DB Size Reached Threshold.....	150
79005 - Avg Bind Size Exceeded.....	151
79105 - Mediation SOAP Too Busy.....	151
79106 - SPR Connection Failed.....	152
79107 - Mediation Disk Quota Exceed.....	152
79108 - Mediation Disk No Space.....	152
79109 - SPR License Limit.....	153
79110 - Stats File Upload Fail.....	153
79120 - Batch Folder Disk Quota Exceeds.....	153
79995 - X1 Connection Lost.....	154
79996 - X2 Connection Lost.....	154
Policy Server Events (80000-89999).....	154
80001 - DB State Transition.....	154
80002 - MySQL Relay Log Dropped.....	155
80003 - QP MySQL DB Level.....	155
82704 - Binding Release Task.....	156
84004 - Policy Info Event.....	156
86001 - Application Is Ready.....	156
86100 - CMP User Login.....	157
86101 - CMP User Login Failed.....	157
86102 - CMP User Logout.....	157
86200 - CMP User Promoted Server.....	158
86201 - CMP User Demoted Server.....	158
86300 - Sh Enable Failed.....	158
86301 - Sh Disable Failed.....	159
86303 - NW-CMP Apply Failed.....	159
86304 - S-CMP Unreachable.....	159
86305 - S-CMP Split Brain.....	160
86306 - CMP Apply Failed.....	160
86307 - S-CMP Sync Fails.....	160
86308 - NCMP Ref Obj Miss.....	161
 Chapter 6: Obtaining SNMP Status and Statistics.....	162
Obtaining CMTS and DPS Connection Status.....	163
Obtaining Rx and Diameter AF Operation Measurement Statistics.....	163
Obtaining PCMM Operation Measurement Statistics.....	165
Glossary.....	167

List of Figures

Figure 1: SNMP Configuration.....	22
Figure 2: Breaker Panel LEDs.....	81
Figure 3: Breaker Panel Setting.....	82
Figure 4: Sample CMTS And DPS Connection Table Statistics.....	163
Figure 5: Sample Rx/Diameter OM Statistics.....	164
Figure 6: Sample PCMM Northbound And Southbound OM Statistics.....	166

List of Tables

Table 1: Admonishments.....	15
Table 2: Alarm and Event Types.....	32

Chapter 1

About This Guide

Topics:

- *How This Guide is Organized.....15*
- *Scope and Audience.....15*
- *Documentation Admonishments.....15*
- *Related Publications.....16*
- *Locate Product Documentation on the Oracle Help Center Site.....16*
- *Customer Training.....16*
- *My Oracle Support (MOS).....17*
- *Emergency Response.....17*

This guide describes Policy Management product support for Simple Network Management Protocol (SNMP).

How This Guide is Organized

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

- [About This Guide](#) contains general information about this guide, the organization of this guide, and how to get technical assistance.
- [Overview](#) provides an overview of how Policy Management supports the Simple Network Management Protocol (SNMP).
- [Configuring SNMP](#) describes how to configure SNMP support on the CMP system.
- [Supported MIBs](#) describes the MIBs that are supported for SNMP.
- [Support for Traps](#) describes Policy Management support of SNMP alarms and traps.
- [Obtaining SNMP Status and Statistics](#) describes support in cable mode for obtaining Diameter Rx and PCMM statistics.




Scope and Audience


This guide is intended for service personnel who are responsible for managing Policy Management systems.

Documentation Admonishments

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

Table 1: Admonishments

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

Icon	Description
	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage.</i>)

Related Publications

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

Locate Product Documentation on the Oracle Help Center Site

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

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

Customer Training

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

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

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Chapter 2

Overview

Topics:

- *Simple Network Management Protocol.....19*
- *The SNMP Standard.....19*

This chapter provides an overview of Policy Management support for the Simple Network Management Protocol (SNMP).

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol that provides a method of managing TCP/IP networks, including individual network devices, and devices in aggregate. SNMP was developed by the IETF (Internet Engineering Task Force), and is applicable to any TCP/IP network, as well as other types of networks.

SNMP is an Application Program Interface (API) to the network, so that general-purpose network management programs can be easily written to work with a variety of different devices. SNMP defines a client/server relationship. The client program (called the network manager) makes virtual connections to a server program (called the SNMP agent). The SNMP agent executes on a remote network device and serves information to the manager about the status of the device. The database (referred to as the SNMP Management Information Base or MIB) is a standard set of statistical and control values that is controlled by the SNMP agent.

Through the use of private MIBs, SNMP allows the extension of the standard values with values specific to a particular agent. SNMP agents can be tailored for a myriad of specific devices such as computers, network bridges, gateways, routers, modems, and printers. The definitions of MIB variables supported by a particular agent are incorporated in descriptor files that are made available to network management client programs so that they can become aware of MIB variables and their usage. The descriptor files are written in Abstract Syntax Notation (ASN.1) format.

Directives are issued by the network manager client to an SNMP agent. Directives consist of the identifiers of SNMP variables (referred to as MIB object identifiers or MIB variables), along with instructions to either get the value for the identifier or set the identifier to a new value.

The SNMP Standard

SNMP can be viewed as three distinct standards:

- A Standard Message Format — SNMP is a standard communication protocol that defines a UDP message format.
- A Standard Set of Managed Objects — SNMP is a standard set of values (referred to as SNMP objects) that can be queried from a device. Specifically, the standard includes values for monitoring TCP, IP, UDP, and device interfaces. Each manageable object is identified with an official name, and also with a numeric identifier expressed in dot-notation.
- A Standard Way of Adding Objects — A standard method is defined to allow the standard set of managed objects to be augmented by network device vendors with new objects specific for a particular network.

SNMP Message Types

Four types of SNMP messages are defined:

- A `get` request returns the value of a named object. Specific values can be fetched to determine the performance and state of the device, without logging into the device or establishing a TCP connection with the device.

- A `get-next` request returns the next name (and value) of the next object supported by a network device given a valid SNMP name. This request allows network managers to review all SNMP values of a device to determine all names and values that an operant device supports.
- A `set` request sets a named object to a specific value. This request provides a method of configuring and controlling network devices through SNMP to accomplish activities such as disabling interfaces, disconnecting users, and clearing registers.
- A `trap` message is generated asynchronously by network devices, which can notify a network manager of a problem apart from any polling of the device. This typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.

The four message types are all encoded into messages referred to as Protocol Data Units (PDUs), which are interchanged with SNMP devices.

Standard Managed Objects

The list of values that an object supports is referred to as the SNMP Management Information Base (MIB). MIB can be used to describe any SNMP object or portion of an SNMP hierarchy.

The various SNMP values in the standard MIB are defined in RFC-1213, one of the governing specifications for SNMP. The standard MIB includes various objects to measure and monitor IP activity, TCP activity, UDP activity, IP routes, TCP connections, interfaces, and general system description. Each of these values is associated with an official name (such as `sysUpTime`, which is the elapsed time since the managed device was booted) and with a numeric value expressed in dot-notation (such as '1.3.6.1.2.1.1.3.0', which is the object identifier for `sysUpTime`).

See [Supported MIBs](#) for a description of the use of SNMP MIBs for Policy Management.

Chapter 3

Configuring SNMP

Topics:

- [About SNMP Configuration.....22](#)
- [Configuring SNMP Settings.....23](#)

This chapter describes how to configure SNMP using the CMP system.

About SNMP Configuration

SNMP configuration architecture is based on using traps to notify a network management system of events and alarms that are generated by the MPE and MRA application software, and those that are generated by the underlying platforms. Alarms and telemetry data are continuously collected from the entire Policy Management network and stored on the CMP system. Alarms will then cause a trap to be sent as a notification of an event.

Because the underlying platform can deliver the alarms from the MPE or MRA system to the CMP system, SNMP can be configured in either of two ways:

- The Policy Management system can be configured so that the CMP system is the source of all traps (the left side of [Figure 1: SNMP Configuration](#)).
- The Policy Management system can be configured to allow each server to generate its own traps and deliver them to the SNMP management servers (the right side of [Figure 1: SNMP Configuration](#)).

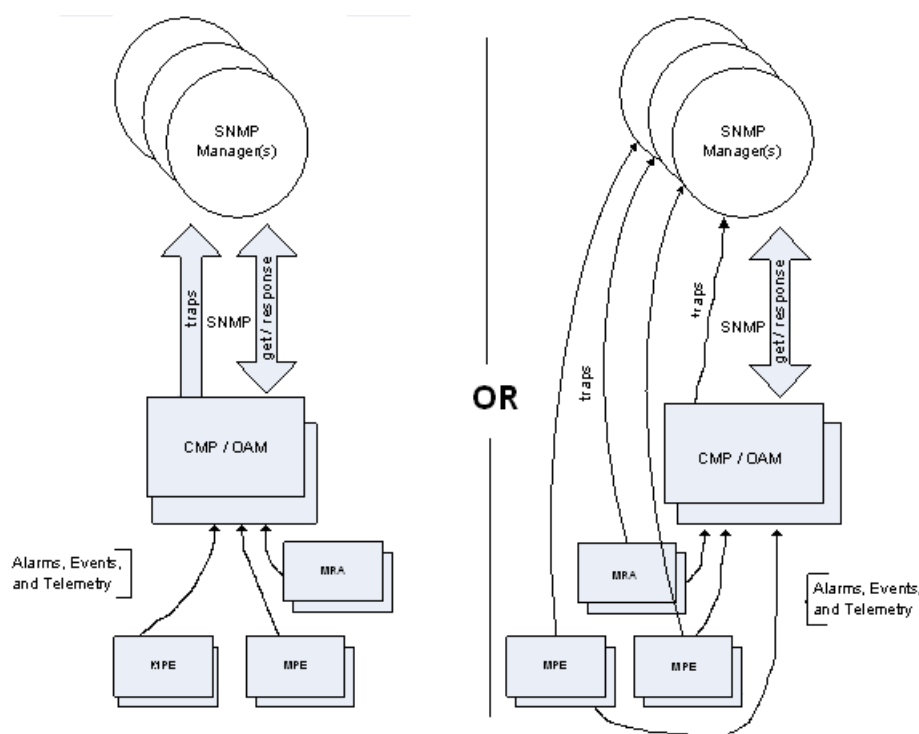


Figure 1: SNMP Configuration

The **Traps from individual Servers** option (see [Configuring SNMP Settings](#)) determines the mode in which the SNMP notifications will operate. When enabled, each server generates traps and the Policy Management system will operate as shown in the right side of [Figure 1: SNMP Configuration](#).

SNMP configuration is pushed from the CMP system to the managed servers in the network.

SNMP Versions

Note: SNMP version 1 (SNMPv1) is not supported.

SNMP version 2c (SNMPv2c) and SNMP version 3 (SNMPv3) are supported. On the **SNMP Setting Edit** page:

- When you configure SNMPv2c, you must use a **Community Name** that is not **public** or **private**.
- When you configure SNMPv3, you must enter an **Engine ID**, a **Username**, and **Password** for the SNMPv3 user.

Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network. You can configure the Policy Management network such that the CMP system collects and forwards all traps, or such that each server generates and delivers its own traps.

Note: SNMP settings configuration must be done on the active server in the primary cluster. A warning displays if the login is not on the active primary CMP system.

To configure SNMP settings:

1. Log in to the CMP system from its server address as a user with administrator privileges.
The navigation pane opens.
2. From the **Platform Setting** section of the navigation pane, select **SNMP Setting**.
The **SNMP Settings** page opens.
3. Click **Modify**.
The **Edit SNMP Settings** page opens.
4. For each **Manager 1-5**, enter a valid host name or an IPv4/IPv6 address.
This field is required for an SNMP Manager to receive traps and send SNMP requests. These fields have the following restrictions:
 - A host name should include only alphanumeric characters.
 - Maximum length is 20 characters.
 - Case insensitive (uppercase and lowercase are treated as the same).
 - This field can contain an IPv4/IPv6 IP address.
 - Port configuration is optional for each manager and it can have a value between 1 and 65535. If this field is left blank, the port defaults to 162.

By default, these fields are blank.

Note: The IPv6 address is not supported.

5. Select the **Enabled Versions** from the list:
 - **SNMPv2c**
 - **SNMPv3**
 - **SNMPv2c and SNMPv3 [default]**
6. Select **Traps Enabled** to enable sending SNMPv2 traps.
The default is enabled. Uncheck the check box to disable sending SNMPv2 traps.

Note: To use the SNMP Trap Forwarding feature, enable this option.

7. Select **Traps from individual Servers** to enable sending traps from each individual server.

The default is disabled. Uncheck the check box to send traps from the active CMP system only.

Note: To use the SNMP Trap Forwarding feature, disable this option.

8. Enter the **SNMPv2c Community Name**.

This is the SNMP read-write community string. This field has the following restrictions:

- The field is required if SNMPv2c is enabled.
- The name can contain alphanumeric characters and cannot exceed 31 characters in length.
- The name cannot be either **private** or **public**.

The default value is **snmppublic**.

9. Enter the **SNMPv3 Engine ID**.

This is the configured Engine ID for SNMPv3. This field has the following restrictions:

- The field is required if SNMPv3 is enabled.
- The Engine ID uses only hexadecimal digits (0-9 and a-f).
- The length can be from 10 to 64 digits.

The default is no value (empty).

10. Select the **SNMPv3 Security Level** (SNMPv3 Authentication and Privacy) from the list:

- **No Auth No Priv** — Authenticate using the **Username**. No Privacy.
- **Auth No Priv** — Authenticate using MD5 or SHA1 protocol.
- **Auth Priv** — [default] Authenticate using MD5 or SHA1 protocol. Encrypt using the AES or DES protocol.

11. Select the **SNMPv3 Authentication Type** (Authentication protocol for SNMPv3) from the list:

- **SHA-1** — Use Secure Hash Algorithm authentication.
- **MD5** — [default] Use Message Digest authentication.

12. Select the **SNMPv3 Privacy Type** (Privacy Protocol for SNMPv3) from the list:

- **AES** — [default] Use Advanced Encryption Standard privacy.
- **DES** — Use Data Encryption Standard privacy.

13. Enter the **SNMPv3 Username**.

This field has the following restrictions:

- The field is required if SNMPv3 is enabled.
- The name must contain alphanumeric characters and cannot exceed 32 characters in length.

The default value is **TekSNMPUser**.

14. Enter the **SNMPv3 Password**.

This value is the Authentication password for SNMPv3 and is also used for `msgPrivacyParameters`. This field has the following restrictions:

- The field is required if SNMPv3 is enabled.
- The length of the password must be between 8 and 64 characters and can include any character.

The default value is **snmpv3password**.

15. Click **Save**.

Chapter 4

Supported MIBs

Topics:

- [Supported MIBs.....27](#)

This chapter describes the MIBs that are supported for SNMP.

Supported MIBs

A Management Information Base (MIB) contains information required to manage a product cluster and the applications it runs. The exact syntax and nature of the parameters are described in the version of each MIB that you are loading on your NMS.

SNMP MIB Objects

To use SNMP effectively, an administrator must become acquainted with the SNMP Management Information Base (MIB), which defines all the values that SNMP is capable of reading or setting.

The SNMP MIB is arranged in a tree-structured fashion, similar in many ways to a disk directory structure of files. The top-level SNMP branch begins with the ISO `internet` directory, which contains four main branches:

- The `mgmt` SNMP branch contains the standard SNMP objects usually supported (at least in part) by all network devices.
- The `private` SNMP branch contains those extended SNMP objects defined by network equipment vendors
- The `experimental` and `directory` SNMP branches, also defined within the `internet` root directory, are usually devoid of any meaningful data or objects.

The tree structure is an integral part of the SNMP standard. However, the most pertinent parts of the tree are the `leaf` objects of the tree that provide actual management data about the device. Generally, SNMP leaf objects can be partitioned into two similar but slightly different types that reflect the organization of the tree structure:

Discrete MIB Objects	Discrete SNMP objects contain one piece of management data. The operator has to know only the name of the object and no other information. Discrete objects often represent summary values for a device, particularly useful for scanning information from the network for the purposes of comparing network device performance. These objects are often distinguished from <code>Table</code> objects by adding a <code>'.0'</code> (dot-zero) extension to their names. (If the <code>'.0'</code> extension is omitted from a leaf SNMP object name, it is always implied.)
Table MIB Objects	Table SNMP objects contain multiple pieces of management data; they allow parallel arrays of information to be supported. These objects are distinguished from Discrete objects by requiring a <code>'.'</code> (dot) extension to their names that distinguishes the particular value being referenced.

By convention, SNMP objects are always grouped in an `Entry` directory, within an object with a `Table` suffix. (The `ifDescr` object described above resides in the `ifEntry` directory contained in the `ifTable` directory.) Several constraints are placed on SNMP objects as follows:

- Each object in the `Entry` directory of a table must contain the same number of elements as other objects in the same `Entry` directory, where instance numbers of all entries are the same. Table objects are always regarded as parallel arrays of data.
- When creating a new `Entry` object, SNMP requires that a value be associated with each table entry in a single SNMP message (single PDU). This means that, to create a row in a table (using an SNMP `set` command), a value must be specified for each element in the row.

- If a table row can be deleted, SNMP requires that at least one object in the entry has a control element that is documented to perform the table deletion. (This applies only if a row can be deleted, which is not necessarily required of an SNMP table.)

The '.' (dot) extension is sometimes referred to as the instance number of an SNMP object. In the case of Discrete objects, this instance number will be zero. In the case of Table objects, this instance number will be the index into the SNMP table.

MIB Object Access Values

Each SNMP object is defined to have a particular access, either read-only, read-write, or write-only, that determines whether the user can read the object value, read and write the object (with a `set` command), or only write the object.

Before any object can be read or written, the SNMP community name must be known. These community names are configured into the system by the administrator, and can be viewed as passwords needed to gather SNMP data. Community names allow reference to portions of the SNMP MIB and object subsets. The purpose of these values is to identify commonality between SNMP object sets, though it is common practice to make these community names obscure to limit access to SNMP capability by outside users.

Compiling MIB Objects

One of the principal components of an SNMP manager is a MIB Compiler, which allows new MIB objects to be added to the management system. When a MIB is compiled into an SNMP manager, the manager is made aware of new objects that are supported by agents on the network. The concept is similar to adding a new schema to a database. The agent is not affected by the MIB compilation (because the agent is already aware of its own objects). The act of compiling the MIB allows the manager to know about the special objects supported by the agent and to access these objects as part of the standard object set.

Typically, when a MIB is compiled into the system, the manager creates new folders or directories that correspond to the objects. These folders or directories can typically be viewed with a MIB Browser, which is a traditional SNMP management tool incorporated into virtually all network management systems. These new objects can often be alarmed or possibly modified to affect the performance of the remote agent.

MIB objects are documented in ASN.1 syntax. The user obtains ASN.1 definitions for a new piece of network equipment or new SNMP agent, transfers this file to the network management system, and runs the management system MIB Compiler to incorporate these definitions into the system. Virtually all agents support the RFC-1213 MIB definitions, and most agents support other definitions as well.

At a minimum, the following MIBs must be compiled into the management station that will be receiving traps from the Policy Management systems in the network. The MIBs must be compiled in the following order:

1. tklc_toplevel.mib
2. COMCOL-TC.mib
3. PCRF-ALARM-MIB.mib
4. NET-SNMP-MIB.txt
5. NET-SNMP-AGENT-MIB.txt
6. TKLC-APP-MIB.txt

Note: The MIB CAMIANT-APP-MIB that was used in release 6.3 is replaced by TKLC-APP-MIB. The OID is changed from .1.3.6.1.4.1.21274.4.1.2.1 to .1.3.6.1.4.1.323.5.3.29.2.1.1.1.

Supported MIBs are available on the installation media or by contacting [My Oracle Support \(MOS\)](#).

MIBs are located on the running system in the following directories:

- /usr/TKLC/TKLCcomcol/cm?././prod/share/snmp/mibs (where ?./ refers to the COMCOL software release that is in use on the system)
COMCOL-TC.mib
- /etc/camiant/snmp/mibs
PCRF-ALARM-MIB.mib
- /usr/TKLC/camiant/subagent/mibs (on MPE devices only)
TKLC-APP-MIB.mib
- /usr/share/snmp/mibs
NET-SNMP-MIB.txt
NET-SNMP-AGENT-MIB.txt
- /usr/TKLC/plat/etc/snmp/mib
tklc_toplevel.mib

Chapter 5

Support for Traps

Topics:

- *Alarms Overview.....31*
- *Platform (31000-32800).....34*
- *QBus Platform (70000-70999).....109*
- *Policy Server Alarms (71000-79999).....127*
- *Policy Server Events (80000-89999).....154*

This chapter describes the SNMP alarms and traps supported by Policy Management systems.

Alarms Overview

Alarms provide information about a system's operational condition, which an operator may need to act upon.

MPE or MRA devices generate Policy Server alarms based on the evaluation of component states and external factors. The servers communicate with each other in a cluster. Each server has a database with merge capabilities to replicate the alarm states to the CMP database. This information is shown on the KPI dashboard or in detailed CMP reports.

As alarms and events are raised on an application or the platform, the SNMP subsystem issues a corresponding trap.

Alarms and Events have the following differences:

- Alarms:
 - Are issued when a Fault is detected
 - Are latched until the Fault is removed (that is, they are explicitly set and cleared)
 - Have a Severity: Critical, Major, Minor
 - Will cause a trap
- Events:
 - Are issued when a Condition is detected (not a Fault)
 - Are not latched (that is they are not explicitly set or cleared)
 - Do not have a Severity (the Severity is actually INFO)
 - Might cause a trap

Separate traps are sent upon raising an alarm and upon clearing an alarm.

Application traps contain the following variable bindings in addition to the `sysOpTime` and `trapID` fields:

- `comcolAlarmSrcNode` - The node that originated the alarm
- `comcolAlarmNumber` - The OID of the alarm and trap
- `comcolAlarmInstance` - An instance is used when the trap is for a physical device such as `disk1`, or `connection diameterPeer 10.15.22.232:33119`
- `comcolAlarmSeverity` - Severity of the alarm: Critical (1), Major (2), Minor (3), Info (4), Clear (5)
- `comcolAlarmText` - A text object that defines the trap
- `comcolAlarmInfo` - An extended text field that adds information to the trap text
- `comcolAlarmGroup` - The group from which the trap originated (such as PCRF or QP)

Refer to the *Policy Management Troubleshooting Reference* for more information about Policy Server alarms and traps.

Note: If you encounter an alarm not in this document, contact [My Oracle Support \(MOS\)](#).

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 Group	The type of alarm that has occurred. For a list of Event types see Alarm and event types .
Description	The reason or cause for the alarm.
Severity	The severity of the alarm. This severity may vary, depending on user-defined and specific application settings.
Instance	
HA Score	The HA impact of the alarm: Normal, Failed, or Degraded.
Auto Clear Seconds	The number of seconds required for the alarm to automatically clear (if applicable).
OID	The alarm identifier that appears in SNMP traps.
Alarm ID	The alarm identifier that is used internally (if applicable).
Recovery	Lists any necessary steps for correcting or preventing the alarm.

Alarm and event types

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

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

Table 2: Alarm and Event Types

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

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

Type Name	Type
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack
SW	Software (generic event type)
TCP	Transmission Control Protocol

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 (31000-32800)

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

31000- S/W fault

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

OID: comcolSwFaultNotify

Recovery:

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

31001 - S/W status

Alarm Group: SW

Description: Program status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSwStatusNotify

Recovery:
No action required.

31002 - Process watchdog failure

Alarm Group: SW

Description: Process watchdog timed out

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolProcWatchdogFailureNotify

Recovery:

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

31003 - Tab thread watchdog failure

Alarm Group: SW

Description: Tab thread watchdog timed out

Severity: Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolThreadWatchdogFailureNotify
Recovery:	
1.	Export event history for the given server and the given process.
2.	Contact My Oracle Support (MOS) .

31100 - Database replication fault

Alarm Group:	SW
Description:	The Database replication process is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbReplicationFaultNotify
Recovery:	
1.	Export event history for the given server and inetsync task.
2.	Contact My Oracle Support (MOS) .

31101 - Database replication to slave failure

Alarm Group:	REPL
Description:	Database replication to a slave Database has failed
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepToSlaveFailureNotify
Recovery:	
1.	Check network connectivity between the affected servers.
2.	If there are no issues with network connectivity, contact My Oracle Support (MOS) .

31102 - Database replication from master failure

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

Recovery:

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

31103 - DB Replication update fault

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

Recovery:

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

31104 - DB Replication latency over threshold

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

OID: comcolDbRepLatencyNotify

Recovery:

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

31105 - Database merge fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeFaultNotify

Recovery:

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

31106 - Database merge to parent failure

Alarm Group: COLL

Description: Database merging to the parent Merge Node has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolDbMergeToParentFailureNotify

Recovery:

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

31107 - Database merge from child failure

Alarm Group: COLL

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

Recovery:

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

31108 - Database merge latency over threshold

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

Recovery:

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

31109 - Topology config error

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

Recovery:

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

31110 - Database audit fault

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

Recovery:

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

31111 - Database merge audit in progress

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

Recovery:

No action required.

31112 - DB replication update log transfer timed out

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

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

31113 - DB replication manually disabled

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

31114 - DB replication over SOAP has failed

Alarm Group:	REPL
Description:	Database replication of configuration data via SOAP has failed
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	3600
OID:	comcolDbReplicationSoapFaultNotify
Recovery:	<ol style="list-style-type: none"> 1. Check network connectivity between the affected servers. 2. If there are no issues with network connectivity, contact My Oracle Support (MOS).

31115 - Database service fault

Alarm Group:	SW
---------------------	----

Description:	The Database service process (idbsvc) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbServiceFaultNotify
Recovery:	
	1. Export event history for the given server and idbsvc task.
	2. Contact My Oracle Support (MOS) .

31116 - Excessive shared memory

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

31117 - Low disk free

Alarm Group:	DISK
Description:	The amount of free disk is below configured thresholds
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolLowDiskFreeNotify
Recovery:	
	1. Remove unnecessary or temporary files from partitions.

2. If there are no files known to be unneeded, contact [My Oracle Support \(MOS\)](#).

31118 - Database disk store fault

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

Recovery:

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

31119 - Database updatelog overrun

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

Recovery:

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

31120 - Database updatelog write fault

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

Auto Clear Seconds: 300
OID: comcolDbUpdateLogWriteFaultNotify
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

31121 - Low disk free early warning

Alarm Group: DISK
Description: The amount of free disk is below configured early warning thresholds
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolLowDiskFreeEarlyWarningNotify
Recovery:
 1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
 2. If there are no files known to be unneeded, contact [My Oracle Support \(MOS\)](#).

31122 - Excessive shared memory early warning

Alarm Group: MEM
Description: The amount of shared memory consumed exceeds configured early warning thresholds
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolExcessiveShMemConsumptionEarlyWarnNotify
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

31123 - Database replication audit command complete

Alarm Group: REPL

Description:	ADIC found one or more errors that are not automatically fixable.
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepAuditCmdCompleteNotify
Recovery:	No action required.

31124 - ADIC error

Alarm Group:	REPL
Description:	An ADIC detected errors
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepAuditCmdErrNotify
Recovery:	Contact My Oracle Support (MOS) .

31125 - Database durability degraded

Alarm Group:	REPL
Description:	Database durability has dropped below configured durability level
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbDurabilityDegradedNotify
Recovery:	<ol style="list-style-type: none"> 1. Check configuration of all servers, and check for connectivity problems between server addresses. 2. If the problem persists, contact My Oracle Support (MOS).

31126 - Audit blocked

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

31127 - DB Replication Audit Complete

Alarm Group:	REPL
Description:	DB replication audit completed
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepAuditCompleteNotify
Recovery:	No action required.

31128 - ADIC Found Error

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

Recovery:

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

31129 - ADIC Found Minor Issue

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

Recovery:

No action required.

31130 - Network health warning

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

Recovery:

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

31131 - DB Ousted Throttle Behind

Alarm Group:	DB
Description:	DB ousted throttle may be affecting processes.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

1. Run 'procshm -o' to identify involved processes.
2. Contact [My Oracle Support \(MOS\)](#) if this alarm persists.

31140 - Database perl fault

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

Recovery:

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

31145 - Database SQL fault

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

Recovery:

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

31146 - DB mastership fault

Alarm Group: SW

Description:	DB replication is impaired due to no mastering process (inetrep/inetrep).
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbMastershipFaultNotify
Recovery:	
	1. Export event history for the given server.
	2. Contact My Oracle Support (MOS) .

31147 - DB upsynclog overrun

Alarm Group:	SW
Description:	UpSyncLog is not big enough for (WAN) replication.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbUpSyncLogOverrunNotify
Recovery:	
	Contact My Oracle Support (MOS) .

31148 - DB lock error detected

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

Recovery:

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

31200 - Process management fault

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

Recovery:

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

31201 - Process not running

Alarm Group:	PROC
Description:	A managed process cannot be started or has unexpectedly terminated
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolProcNotRunningNotify

Recovery:

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

31202 - Unkillable zombie process

Alarm Group:	PROC
Description:	A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. Contact [My Oracle Support \(MOS\)](#).

31206 - Process mgmt monitoring fault

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

Recovery:

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

31207 - Process resource monitoring fault

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

Recovery:

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

31208 - IP port server fault

Alarm Group: SW

Description:	The run environment port mapper (re.portmap) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolPortServerFaultNotify
Recovery:	Contact My Oracle Support (MOS) .

31209 - Hostname lookup failed

Alarm Group:	SW
Description:	Unable to resolve a hostname specified in the NodeInfo table
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHostLookupFailedNotify
Recovery:	<ol style="list-style-type: none"> 1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm. 2. If the problem persists, contact My Oracle Support (MOS).

31213 - Process scheduler fault

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

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

31214 - Scheduled process fault

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

Recovery:

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

31215 - Process resources exceeded

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

Recovery:

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

31216 - SysMetric configuration error

Alarm Group:	SW
Description:	A SysMetric Configuration table contains invalid data
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300

OID: comcolSysMetricConfigErrorNotify

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

31220 - HA configuration monitor fault

Alarm Group: SW

Description: The HA configuration monitor is impaired by a s/w fault.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaCfgMonitorFaultNotify

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

31221 - HA alarm monitor fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAlarmMonitorFaultNotify

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

31222 - HA not configured

Alarm Group: HA

Description: High availability is disabled due to system configuration

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300
OID: comcolHaNotConfiguredNotify
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

31223 - HA Heartbeat transmit failure

Alarm Group: HA
Description: The high availability monitor failed to send heartbeat.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaHbTransmitFailureNotify
Recovery:

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

31224 - HA configuration error

Alarm Group: HA
Description: High availability configuration error
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaCfgErrorNotify
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

31225 - HA service start failure

Alarm Group: HA
Description: The required high availability resource failed to start.
Severity: Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0
OID:	comcolHaSvcStartFailureNotify

Recovery:

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

31226 - HA availability status degraded

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

Recovery:

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

31227 - HA availability status failed

Alarm Group:	HA
Description:	The high availability status is failed due to raised alarms.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaAvailFailedNotify

Recovery:

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

31228 - HA standby offline

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

Recovery:

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

31229 - HA score changed

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

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

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

Auto Clear Seconds: 300
OID: comcolRecAlarmEvProcFaultNotify

Recovery:

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

31231 - Platform alarm agent fault

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

Recovery:

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

31232 - Late heartbeat warning

Alarm Group: HA
Description: High availability server has not received a message on specified path within the configured interval.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaLateHeartbeatWarningNotify

Recovery:

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

31233 - HA Path Down

Alarm Group: HA
Description: High availability path loss of connectivity

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

Recovery:

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

31234 - Untrusted Time Upon Initialization

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

Recovery:

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

31235 - Untrusted Time After Initialization

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

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

Recovery:

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

31236 - HA Link Down

Alarm Group:	HA
Description:	High availability TCP link is down.
Severity:	Critical
Instance:	Remote node being connected to plus the path identifier
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaLinkDownNotify

Recovery:

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

31240 - Measurements collection fault

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

Recovery:

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

31250 - RE port mapping fault

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

Recovery:

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

31260 - SNMP Agent

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

Recovery:

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

31270 - Logging output

Alarm Group:	SW
Description:	Logging output set to Above Normal
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

Extra diagnostic logs are being collected, potentially degrading system performance. Contact [My Oracle Support \(MOS\)](#).

31280 - HA Active to Standby transition

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

Recovery:

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

31281 - HA Standby to Active transition

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

Recovery:

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

31282 - HA Management Fault

Alarm Group: HA

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

Recovery:

Export event history for the given server and cmha task, then Contact [My Oracle Support \(MOS\)](#).

31283 - Lost Communication with server

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

Recovery:

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

31284 - HA Remote Subscriber Heartbeat Warning

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

Recovery:

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

31285 - HA Node Join Recovery Entry

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

Recovery:

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

31286 - HA Node Join Recovery Plan

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

Recovery:

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

31287 - HA Node Join Recovery Complete

Alarm Group:	HA
Description:	High availability node join recovery complete
Severity:	Info
Instance:	Names of HA Policies (as defined in HA policy configuration)

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

Recovery:

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

31290 - HA Process Status

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

Recovery:

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

31291 - HA Election Status

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

Recovery:

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

31292 - HA Policy Status

Alarm Group:	HA
---------------------	----

Description:	HA Policy plan status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaPolicyStatusNotify
Recovery:	
	1. If this alarm occurs during routine maintenance activity, it may be ignored.
	2. Otherwise, contact My Oracle Support (MOS) .

31293 - HA Resource Link Status

Alarm Group:	HA
Description:	HA ResourceAgent Link status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaRaLinkStatusNotify
Recovery:	
	1. If this alarm occurs during routine maintenance activity, it may be ignored.
	2. Otherwise, contact My Oracle Support (MOS) .

31294 - HA Resource Status

Alarm Group:	HA
Description:	HA Resource registration status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaResourceStatusNotify
Recovery:	
	1. If this alarm occurs during routine maintenance activity, it may be ignored.

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

31295 - HA Action Status

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

Recovery:

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

31296 - HA Monitor Status

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

Recovery:

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

31297 - HA Resource Agent Info

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

OID: comcolHaRaInfoNotify

Recovery:

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

31298 - HA Resource Agent Detail

Alarm Group: HA

Description: Resource Agent application detailed information

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaDetailNotify

Recovery:

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

31299 - HA Notification Status

Alarm Group: HA

Description: HA Notification status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaNotificationNotify

Recovery:

No action required.

31300 - HA Control Status

Alarm Group: HA

Description: HA Control action status

Severity: Info

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

31301 - HA Topology Events

Alarm Group:	HA
Description:	HA Topology events
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	eagleXgDsrHaTopologyNotify
Recovery:	No action required.

32113 - Uncorrectable ECC memory error

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

32114 - SNMP get failure

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

Recovery:

1. Use the following command to verify the switch is active: `ping switch1A/B` (this requires command line access).
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32115 - TPD NTP Daemon Not Synchronized Failure

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

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32116 - TPD Server's Time Has Gone Backwards

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

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

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32117 - TPD NTP Offset Check Failure

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

Recovery:

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

32300 - Server fan failure

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

Alarm ID: TKSPLATMA1

Recovery:

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

32301 - Server internal disk error

Alarm Group: PLAT

Description: This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdIntDiskError

Alarm ID: TKSPLATMA2

Recovery:

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

32303 - Server Platform error

Alarm Group: PLAT

Description: This alarm indicates an error such as a corrupt system configuration or missing files.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPlatformError

Alarm ID: TKSPLATMA4

Recovery:

Contact [My Oracle Support \(MOS\)](#) and provide the system health check output.

32304 - Server file system error

Alarm Group: PLAT

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

32305 - Server Platform process error

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

32307 - Server swap space shortage failure

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

Auto Clear Seconds: 0 (zero)
OID: tpdSwapSpaceShortageError
Alarm ID: TKSPLATMA8
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32308 - Server provisioning network error

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

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


32312 - Server disk space shortage error

Alarm Group: PLAT
Description: This alarm indicates that one of the following conditions has occurred:

- A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system.
- More than 90% of the total number of available files have been allocated on the file system.
- A file system has a different number of blocks than it had when installed.

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

32313 - Server default route network error

Alarm Group:	PLAT
Description:	This alarm indicates that the default network route of the server is experiencing a problem.
<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>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.</p> </div> </div>	
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDefaultRouteNetworkError
Recovery:	Contact My Oracle Support (MOS) .

32314 - Server temperature error

Alarm Group:	PLAT
Description:	The internal temperature within the server is unacceptably high.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerTemperatureError
Alarm ID:	TKSPLATMA15

Recovery:

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

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

3. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#).

32315 - Server mainboard voltage error

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

Recovery:

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

32316 - Server power feed error

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

Auto Clear Seconds: 0 (zero)
OID: tpdPowerFeedError
Alarm ID: TKSPLATMA17

Recovery:

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

32317 - Server disk health test error

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

Recovery:

1. Perform the recovery procedures for the other alarms that accompany this alarm.
2. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#).

32318 - Server disk unavailable error

Alarm Group:	PLAT
Description:	The smartd service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskUnavailableError
Alarm ID:	TKSPLATMA19
Recovery:	Contact My Oracle Support (MOS) .

32320 - Device interface error

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

32321 - Correctable ECC memory error

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

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

Recovery:

No recovery necessary. If the condition persists, contact [My Oracle Support \(MOS\)](#) to request hardware replacement.

32322 - Power Supply A error

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

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32323 - Power Supply B error

Alarm Group:	PLAT
Description:	This alarm indicates that power supply 2 (feed B) has failed.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdPowerSupply2Error
Alarm ID:	TKSPLATMA24

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

32324 - Breaker panel feed error

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

Recovery:

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

32325 - Breaker panel breaker error

Alarm Group:	PLAT
Description:	<p>This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see Figure 2: Breaker Panel LEDs) identify whether the fault occurred on the input power or the output power, as follows:</p> <ul style="list-style-type: none"> • A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit. <p>Note: LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.</p>

- A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.

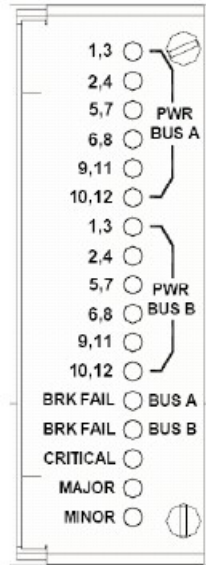


Figure 2: Breaker Panel LEDs

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	TPDBrkPnlBreakerError
Alarm ID:	TKSPLATMA26

Recovery:

1. Verify that the same alarm is displayed by multiple servers:
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by multiple servers, go to the next step.
2. Look at the breaker panel assignments and verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

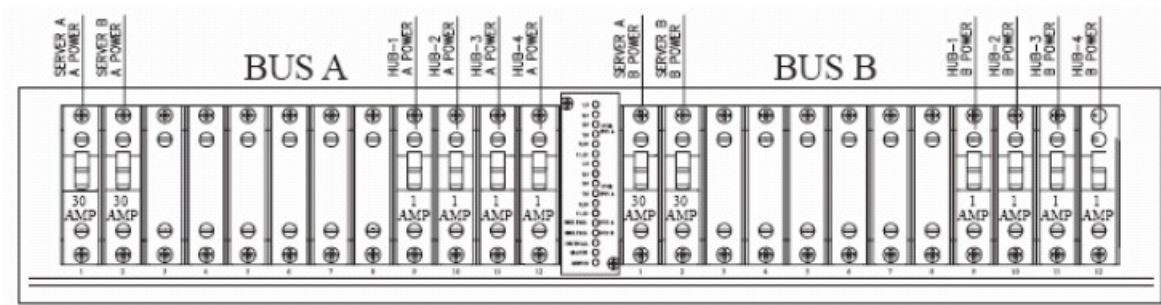


Figure 3: Breaker Panel Setting

If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Contact [My Oracle Support \(MOS\)](#)

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 [My Oracle Support \(MOS\)](#)
 - If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, continue with the next step.
 - If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise Contact [My Oracle Support \(MOS\)](#)
4. If the problem has not been resolved, contact [My Oracle Support \(MOS\)](#)

32326 - Breaker panel monitoring error

Alarm Group: PLAT

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

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

- 32324 – Breaker panel feed error

- 32325 – Breaker panel breaker error

until the Breaker Panel Monitoring Error has been corrected.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdBrkPnlMntError
Alarm ID:	TKSPLATMA27

Recovery:

1. Verify that the same alarm is displayed by multiple servers:
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).
3. If the alarm has not been cleared, contact [My Oracle Support \(MOS\)](#).

32327 - Server HA Keepalive error

Alarm Group:	PLAT
Description:	This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaKeepaliveError
Alarm ID:	TKSPLATMA28

Recovery:

1. Determine if the mate server is currently down and bring it up if possible.
2. Determine if the keepalive interface is down.
3. Determine if heartbeat is running (service TKLCha status).

Note: This step may require command line ability.
4. Contact [My Oracle Support \(MOS\)](#).

32331 - HP disk problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with either a physical or logical disk in the HP disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskProblem
Alarm ID:	TKSPLATMA32
Recovery:	Contact My Oracle Support (MOS) .

32332 - HP Smart Array controller problem

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

32333 - HP hpacucliStatus utility problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that

	the hpacucliStatus/hpDiskStatus daemon is either not running, or hung.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHPACUCLIPProblem
Alarm ID:	TKSPLATMA34
Recovery:	Contact My Oracle Support (MOS) .

32335 - Switch link down error

Alarm Group:	PLAT
Description:	The link is down.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSwitchLinkDownError
Alarm ID:	TKSPLATMA36
Recovery:	<ol style="list-style-type: none"> 1. Verify the cabling between the port and the remote side. 2. Verify networking on the remote end. 3. If the problem persists, contact My Oracle Support (MOS) who should verify port settings on both the server and the switch.

32336 - Half Open Socket Limit

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

Auto Clear Seconds: 0 (zero)
OID: tpdHalfOpenSockLimit
Alarm ID: TKSPLATMA37
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32337 - Flash Program Failure

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

32338 - Serial Mezzanine Unseated

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

1. Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.
2. Contact My Oracle Support (MOS) if reseating the cables does not clear the alarm.

32339 - Max pid limit

Alarm Group:	PLAT
Description:	This alarm indicates that the maximum number of running processes has reached the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdMaxPidLimit
Alarm ID:	TKSPLATMA40
Recovery:	Contact My Oracle Support (MOS) .

32340 - Server NTP Daemon Lost Synchronization For Extended Time

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedError
Alarm ID:	TKSPLATMA41
Recovery:	<ol style="list-style-type: none"> 1. Verify NTP settings and that NTP sources can be reached. 2. Contact My Oracle Support (MOS).

32341 - Server NTP Daemon Never Synchronized Error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.
Severity:	Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNeverSynchronized
Alarm ID:	TKSPLATMA42

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. Contact [My Oracle Support \(MOS\)](#).

32342 - NTP Offset Check Error

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

Recovery:

1. Verify NTP settings and that NTP are providing accurate time.
2. Contact [My Oracle Support \(MOS\)](#).

32343 - RAID disk problem

Alarm Group:	PLAT
Description:	This alarms indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskProblem
Alarm ID:	TKSPLATMA44

Recovery:

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

32344 - RAID controller problem

Alarm Group:	PLAT
Description:	This alarms indicates that RAID controller needs intervention.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskCtrlrProblem
Alarm ID:	TKSPLATMA45

Recovery:

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

32345 - Server Upgrade snapshot(s) invalid

Alarm Group:	PLAT
Description:	This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdUpgradeSnapshotInvalid
Alarm ID:	TKSPLATMA46

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. Contact [My Oracle Support \(MOS\)](#)

32346 - Server Hardware Problem

Alarm Group:	PLAT
Description:	This alarms indicates that OEM hardware management service reports an error.

Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdOEMHardware
Alarm ID:	TKSPLATMA47
Recovery:	Contact My Oracle Support (MOS)

32347 - Oracle hwmgmtcliStatus Problem

Alarm Group:	PLAT
Description:	This alarms indicates the hwmgmtcliStatus daemon is not running or is not responding.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHWMGMTCLIPProblem
Alarm ID:	TKSPLATMA47
Recovery:	Contact My Oracle Support (MOS)

32348 - FIPS subsystem problem

Alarm Group:	PLAT
Description:	This alarm indicates the FIPS subsystem is not running or has encountered errors.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdFipsSubsystemProblem
Recovery:	

1. Run syscheck in verbose mode.
2. Contact [My Oracle Support \(MOS\)](#).

32349 - File Tampering

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

32350 - Security Process Terminated

Alarm Group:	PLAT
Description:	This alarm indicates that the security process monitor is not running.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSecurityProcessDown
Recovery:	Contact My Oracle Support (MOS) .

32500 - Server disk space shortage warning

Alarm Group:	PLAT
Description:	<p>This alarm indicates that one of the following conditions has occurred:</p> <ul style="list-style-type: none"> • A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system. • More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskSpaceShortageWarning
Alarm ID:	TKSPLATMI1
Recovery:	Contact My Oracle Support (MOS) .

32501 - Server application process error

Alarm Group:	PLAT
Description:	This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdApplicationProcessError
Alarm ID:	TKSPLATMI2
Recovery:	Contact My Oracle Support (MOS) .

32502 - Server hardware configuration error

Alarm Group:	PLAT
Description:	This alarm indicates that one or more of the server's hardware components are not in compliance with specifications (refer to the appropriate hardware manual).
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHardwareConfigError

Alarm ID: TKSPLATMI3

Recovery:

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

32505 - Server swap space shortage warning

Alarm Group: PLAT

Description: This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

Note: For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSwapSpaceShortageWarning

Alarm ID: TKSPLATMI6

Recovery:

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

32506 - Server default router not defined

Alarm Group: PLAT

Description: This alarm indicates that the default network route is either not configured or the current configuration contains an invalid IP address or hostname.



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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)
OID: tpdDefaultRouteNotDefined
Alarm ID: TKSPLATMI7
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32507 - Server temperature warning

Alarm Group: PLAT
Description: This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdServerTemperatureWarning
Alarm ID: TKSPLATMI8

Recovery:

1. Ensure that nothing is blocking the fan'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 [My Oracle Support \(MOS\)](#).

32508 - Server core file detected

Alarm Group: PLAT
Description: This alarm indicates that an application process has failed and debug information is available.
Severity: Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerCoreFileDetected
Alarm ID:	TKSPLATMI9

Recovery:

1. Contact [My Oracle Support \(MOS\)](#) to create a service request.
2. On the affected server, execute this command:

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

Add the command output to the service request. Include the date of creation found in the command output.

3. Attach core files to the MOS service request.
4. The user can remove the files to clear the alarm with this command:

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

32509 - Server NTP Daemon not synchronized

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

Recovery:

1. Locate the server's Network Timing Protocol (NTP) source.
2. Determine if the NTP server is reachable.
3. Contact [My Oracle Support \(MOS\)](#) if additional assistance is needed.

32510 - CMOS battery voltage low

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

Description:	The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdCMOSBatteryVoltageLow
Alarm ID:	TKSPLATMI11
Recovery:	Contact My Oracle Support (MOS) .

32511 - Server disk self test warning

Alarm Group:	PLAT
Description:	A non-fatal disk issue (such as a sector cannot be read) exists.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSmartTestWarn
Alarm ID:	TKSPLATMI12
Recovery:	Contact My Oracle Support (MOS) .

32512 - Device warning

Alarm Group:	PLAT
Description:	This alarm indicates that either we are unable to perform an snmpget command on the configured SNMP OID or the value returned failed the specified comparison operation.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds: 0 (zero)
OID: tpdDeviceWarn
Alarm ID: TKSPLATMI13

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

32513 - Device interface warning

Alarm Group: PLAT
Description: This alarm can be generated by either an SNMP trap or an IP bond error.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdDeviceIfWarn
Alarm ID: TKSPLATMI14

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

32514 - Server reboot watchdog initiated

Alarm Group: PLAT
Description: This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdWatchdogReboot
Alarm ID: TKSPLATMI15

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

32515 - Server HA failover inhibited

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

32516 - Server HA Active to Standby transition

Alarm Group:	PLAT
Description:	This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaActiveToStandbyTrans
Alarm ID:	TKSPLATMI17
Recovery:	Contact My Oracle Support (MOS) .

32517 - Server HA Standby to Active transition

Alarm Group:	PLAT
Description:	This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdHaStandbyToActiveTrans
Alarm ID: TKSPLATMI18
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32518 - Platform Health Check failure

Alarm Group: PLAT
Description: This alarm is used to indicate a configuration error.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdHealthCheckFailed
Alarm ID: TKSPLATMI19
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32519 - NTP Offset Check failure

Alarm Group: PLAT
Description: This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the NTP server and the offset limit that the application has set for the system.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: ntpOffsetCheckWarning
Alarm ID: TKSPLATMI20
Recovery:
 Contact [My Oracle Support \(MOS\)](#).

32520 - NTP Stratum Check failure

Alarm Group:	PLAT
Description:	This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	ntpStratumCheckFailed
Alarm ID:	TKSPLATMI21

Recovery:

1. Locate the server's Network Timing Protocol (NTP) source.
2. Check the NTP server's stratum level. Stratum level 13 or higher will generate the alarm.
3. Contact [My Oracle Support \(MOS\)](#) if additional assistance is needed.

32521 - SAS Presence Sensor Missing

Alarm Group:	PLAT
Description:	This alarm indicates that the T1200 server drive sensor is not working.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	sasPresenceSensorMissing
Alarm ID:	TKSPLATMI22

Recovery:

Contact [My Oracle Support \(MOS\)](#) to get a replacement server.

32522 - SAS Drive Missing

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

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	sasDriveMissing
Alarm ID:	TKSPLATMI23
Recovery:	Contact My Oracle Support (MOS) to determine whether the issue is with a failed drive or failed configuration.

32524 - HP disk resync

Alarm Group:	PLAT
Description:	This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskResync
Alarm ID:	TKSPLATMI25
Recovery:	Contact My Oracle Support (MOS) .

32525 - Telco Fan Warning

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

HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoFanWarning
Alarm ID:	TKSPLATMI26

Recovery:

1. Contact [My Oracle Support \(MOS\)](#) to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.
2. [My Oracle Support \(MOS\)](#) personnel can perform an snmpget command or log into the switch to get detailed fan status information.

32526 - Telco Temperature Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoTemperatureWarning
Alarm ID:	TKSPLATMI27

Recovery:

1. Lower the ambient air temperature around the switch as low as possible.
2. If problem persists, contact [My Oracle Support \(MOS\)](#).

32527 - Telco Power Supply Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoPowerSupplyWarning
Alarm ID:	TKSPLATMI28

Recovery:

1. Verify breaker wasn't tripped.
2. If breaker is still good and problem persists, contact [My Oracle Support \(MOS\)](#) who can perform a `snmpget` command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 - Invalid BIOS value

Alarm Group:	PLAT
Description:	This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdInvalidBiosValue
Alarm ID:	TKSPLATMI29

Recovery:

Change the BIOS values to the expected values which involves re-booting the server. Contact [My Oracle Support \(MOS\)](#) for directions on changing the BIOS.

32529 - Server Kernel Dump File Detected

Alarm Group:	PLAT
Description:	This alarm indicates that the kernel has crashed and debug information is available.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerKernelDumpFileDetected
Alarm ID:	TKSPLATMI30

Recovery:

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

32530 - Server Upgrade Fail Detected

Alarm Group:	PLAT
Description:	This alarm indicates that a TPD upgrade has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	pdServerUpgradeFailed
Alarm ID:	TKSPLATMI31
Recovery:	Contact My Oracle Support (MOS) .

32531 - Half Open Socket Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHalfOpenSocketWarning
Alarm ID:	TKSPLATMI32
Recovery:	Contact My Oracle Support (MOS) .

32532 - Server Upgrade Pending Accept/Reject

Alarm Group:	PLAT
Description:	This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdServerUpgradePendingAccept
Alarm ID: TKSPLATMI33

Recovery:

Follow the steps in the application's upgrade procedure for accepting or rejecting the upgrade.

32533 - Max pid warning

Alarm Group: PLAT
Description: This alarm indicates that the maximum number of running processes has reached the minor threshold.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdMaxPidWarning
Alarm ID: TKSPLATMI34

Recovery:

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

32534 - NTP Source Server Is Not Able To Provide Correct Time

Alarm Group: PLAT
Description: This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdNTPSourceIsBad
Alarm ID: TKSPLATMI35

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. Contact [My Oracle Support \(MOS\)](#).

32535 - RAID disk resync

Alarm Group:	PLAT
Description:	This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskResync
Alarm ID:	TKSPLATMI36
Recovery:	If this alarm persists for several hours (depending on a load of a server rebuild of array can take multiple hours to finish), contact My Oracle Support (MOS) .

32536 - Server Upgrade snapshot(s) warning

Alarm Group:	PLAT
Description:	This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdUpgradeSnapshotWarning
Alarm ID:	TKSPLATMI37
Recovery:	<ol style="list-style-type: none"> 1. Run accept or reject of current LVM upgrade before snapshots become invalid. 2. Contact My Oracle Support (MOS)

32540 - Power limit mismatch

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

32700 - Telco Switch Notification

Alarm Group:	PLAT
Description:	Telco Switch Notification
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	86400
OID:	tpdTelcoSwitchNotification
Recovery:	Contact My Oracle Support (MOS) .

32701 - HIDS Initialized

Alarm Group:	PLAT
Description:	This alarm indicates HIDS was initialized.
Default Severity:	Info
OID:	tpdHidsBaselineCreated
Recovery:	Contact My Oracle Support (MOS) .

32702 - HIDS Baseline Deleted

Alarm Group:	PLAT
Description:	HIDS baseline was deleted.
Default Severity:	Info
OID:	tpdHidsBaselineDeleted
Recovery:	
Contact My Oracle Support (MOS) .	

32703 - HIDS Enabled

Alarm Group:	PLAT
Description:	HIDS was enabled.
Default Severity:	Info
OID:	tpdHidsEnabled
Recovery:	
Contact My Oracle Support (MOS) .	

32704 - HIDS Disabled

Alarm Group:	PLAT
Description:	HIDS was disabled.
Default Severity:	Info
OID:	tpdHidsDisabled
Recovery:	
Contact My Oracle Support (MOS) .	

32705 - HIDS Monitoring Suspended

Alarm Group:	PLAT
Description:	HIDS monitoring suspended.
Default Severity:	Info
OID:	tpdHidsSuspended
Recovery:	
Contact My Oracle Support (MOS) .	

32706 - HIDS Monitoring Resumed

Alarm Group:	PLAT
Description:	HIDS monitoring resumed.
Default Severity:	Info
OID:	tpdHidsResumed
Recovery:	Contact My Oracle Support (MOS) .

32707 - HIDS Baseline Updated

Alarm Group:	PLAT
Description:	HIDS baseline updated.
Default Severity:	Info
OID:	tpdHidsBaselineUpdated
Recovery:	Contact My Oracle Support (MOS) .

QBus Platform (70000-70999)

The QBus Platform (QP) software provides an execution environment for Java-based applications, which are the Multiprotocol Routing Agent (MRA) devices, Multimedia Policy Engine (MPE) devices, or the Configuration Management Platform (CMP) server. QP provides common interfaces into databases, event logging, SNMP, and cluster state. Two servers in the cluster provide 1+1 High-Availability (HA) protection. The application executes on one server. The other server acts as a hot standby in case the first server 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	QPProcmgrFailed

Recovery:

If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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 clears automatically.
OID	QPCriticalProcFailed

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

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	QPNonCriticalProcFailed

Recovery:

1. If the alarm occurs infrequently, monitor the health of the system.
2. If the alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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	QPMaintShutdown
Recovery:	
	If the alarm is occurring, confirm that the server is down for maintenance.

70005 – QP Cluster Status

Alarm Type	QP
Description	One or more servers in the cluster are not at QP Blade Status. The QP Blade Status is not available for one or more servers in the cluster.
Default Severity	Major Critical
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears when all server blades have QP blade status of Available.
OID	QPClusterStatus
Recovery:	
	If the alarm occurs infrequently, monitor the health of the system. If the alarm occurs frequently, contact My Oracle Support (MOS) .

70006 - QP Blade Status

Alarm Type:	PLAT
Description	This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive or another change in the configuration. The output of the message includes the disk that is resyncing. This alarm eventually clears 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 (rebuild of 600G disks without any load takes about 75min).
Default Severity	Minor
Instance	N/A
HA Score	N/A
Clearing Action	N/A
OID	tpdNTPSourceIsBad
Recovery:	

1. Run syscheck in verbose mode.
2. If this alarm persist for several hours (Server rebuild of the array may take multiple hours to finish, depending on the load of the server), contact [My Oracle Support \(MOS\)](#).

70008 - QP Database Service Failed

Alarm Type:	PLAT
Description	This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive or another change in the configuration. The output of the message includes the disk that is resyncing. This alarm eventually clears 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 (rebuild of 600G disks without any load takes about 75min).
Default Severity:	Minor
Instance	N/A
HA Score	N/A
Clearing Action	N/A
OID	tpdNTPSourceIsBad

Recovery:

1. Run syscheck in verbose mode.
2. If this alarm persist for several hours (Server rebuild of the array may take multiple hours to finish, depending on the load of the server), contact [My Oracle Support \(MOS\)](#).

70009 – QP Topology Configuration Mismatch

Alarm Type	QP
Description	<p>The running topology does not match the saved topology. The qp_procmgr has detected that its Topology configuration (topology or VIP) does not match the configuration in the database.</p> <p>Running cluster configuration:</p> <ul style="list-style-type: none"> • Topology={Undefined, Unmated, Mated} • Mate={x.x.x.x} • OAM VIP={x.x.x.x} • SIG-A VIP={x.x.x.x}, • SIG-B VIP={x.x.x.x}
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	qp_procmgr exit
OID	QPTopologyConfigurationMismatch

Recovery:

Restart the `qp_procmgr` service either through a full restart or becoming root and performing `service qp_procmgr restart`.

70010 – QP Failed Server-backup Remote Archive Rsync

Alarm Type	QP
Description	<p>A scheduled backup failed to synchronize the local server-backup archive with the remote server-backup archive.</p> <ul style="list-style-type: none"> • Hostname=<hostname IPaddr> • path=<path> • errorcode=<rsync error>
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 64800 seconds (18 hours).
OID	QPServerBackupRsyncFailed

Recovery:

Check that the parameters are correct.

70011 – QP Failed System-backup Remote Archive Rsync

Alarm Type	QP
Description	<p>A scheduled backup failed to synchronize the local system-backup archive with the remote system-backup archive.</p> <p>Hostname=<host name IP addr>, user=<user>, path=<path>,errorcode=<rsync error></p>
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 64800 seconds (18 hours).
OID	QPSystemBackupRsyncFailed

Recovery:

Check that the parameters are correct.

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 64800 seconds (18 hours).
OID	QPServerBackupFailed

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 64800 seconds (18 hours).
OID	QPSystemBackupFailed

Recovery:

Take corrective action based on the returned error message.

70015 – 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: <ul style="list-style-type: none"> • 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 (60 minutes).
OID	QpAddRouteFailed

Recovery:

Use Platcfg Routing menu to repair the route manually.

70016 – No Available VIP Route

Alarm Type	QP
Description	This alarm is raised when the application of a route item with VIP as the preferred source fails because the VIP is not configured.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	When VIP becomes available, this alarm is cleared. If the route item is deleted, this alarm is also cleared.
OID	QPNoVipForRoute

Recovery:

1. Check route configuration.
2. If route is configured correctly, this alarm can be ignored.

70017 – No Available Static IP

Alarm Type	QP
Description	This alarm is raised when the application of a route item with STATIC IP as preferred source fails because the STATIC IP is not available.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	When a STATIC IP becomes available, this alarm is cleared. If the route item is deleted, this alarm is also cleared.
OID	QPNoStaticIPForRoute

Recovery:

1. Check the network connectivity between SMSR and configured destination.
2. Check route configuration; if route is configured correctly, this alarm can be ignored.

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	QPMysqlMasterOutdated

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 restart and its DB Level will not be known until after the restart 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 forced standby.
4. If the best slave is in the same cluster (the most common case), 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	QPMysqlSlaveUnconnected

Recovery:

1. No action required unless the alarm does not clear within a few hours.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

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	QPMysqlSlaveSyncFailure

Recovery:

1. No action required unless the alarm does not clear within a few hours.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

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	QPMysqlSlaveLagging

Recovery:

1. No action required unless the alarm does not clear within a few hours or the condition is repeatedly set and cleared.
2. If either of the problems persists, contact [My Oracle Support \(MOS\)](#).

70024 - QP Slave database is prevented from synchronizing with the master

Alarm Type	QP
Description	The MySQL slave has been prevented from synchronizing 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	QPMysqlSlaveSyncPrevented

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. 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.
Default Severity	Critical
Instance	N/A
HA Score	DegradedNormal
Clearing Action	The slave server clears the alarm when the master DB version is equal to the slave DB version.
OID	QPMysqlSchemaVersionMismatch

Recovery:

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	QPNetBackupInProgress

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

70028 – QP bonded interface is down

Alarm Type	QP
Description	OAM bonded interface bond0 is down; Signaling bonded interface bond1 is down; Signaling bonded interface bond2 is down.
Default Severity	Critical
Instance	OAM, SIGA, SIGB
HA Score	Degraded
Clearing Action	Process <code>qp_hamonitor</code> has detected the VIP is not defined on this bonded network interface; VIP is defined on this bonded network interface and <code>qp_hamonitor</code> process has detected the interface is up
OID	QPBondedInterfaceDown

Recovery:

If the alarm does not clear within a few seconds automatically or if the alarm is occurring over and over, contact [My Oracle Support \(MOS\)](#).

70029 – QP peer node bonded interface is down

Alarm Type	QP
Description	QP Peer Node <i>\${host name}</i> (<i>\${ip addr}</i>) bonded interface bond0 (OAM) is down.
Default Severity	Critical
Instance	Peer_OAM
HA Score	Normal
Clearing Action	Process <code>qp_hamonitor</code> has detected the OAM network interface is up or alarm has been raised for 60 seconds.
OID	QPPeerBondedInterfaceDown

Recovery:

If the alarm does not clear within a few seconds automatically or if the alarm is occurring over and over, contact [My Oracle Support \(MOS\)](#).

70030 – QP backplane bonded interface is down

Alarm Type	QP
------------	----

Description	Backplane bonded interface bond3 is down.
Default Severity	Critical
Instance	Backplane_bond3
HA Score	Normal
Clearing Action	Process <code>qp_hamonitor</code> has detected the bonded backplane network interface is up or alarm has been raised for 60 seconds.
OID	QPSBackplaneBondedInterfaceDown

Recovery:

If the alarm does not automatically clear within a few seconds or if the alarm is occurring over and over, contact [My Oracle Support \(MOS\)](#).

70031 – QP degrade because one or more interfaces are down

Alarm Type	QP
Description	HA status is degraded because selected interface(s) (<i>OAM, SIGA, or SIGB</i>) are down.
Default Severity	Critical
Instance	OAM or SIGA or SIGB
HA Score	Failed
Clearing Action	Process <code>qp_hamonitor</code> has detected all OAM, SIGA and SIGB network interfaces are up, or alarm has been raised for 60 seconds.
OID	QPInterfacesDegrade

Recovery:

If the alarm does not automatically clear within a few seconds or if the alarm is occurring over and over, contact [My Oracle Support \(MOS\)](#).

70032 – QP direct link does not work as configuration

Alarm Type	QP
Description	QP degrade because one or more interfaces are down. This alarm is due to the incorrect configuration of backplane so that it cannot be applied to the system.
Default Severity	Notice
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	QPBpMismatch

Recovery:

Check the validity of backplane IP Address and Comcol table LogicPath.

70038 – QP has blocked IPv4 traffic on an OAM interface

Alarm Type	QP
Description	This alarm is raised on each server if IPv4 is blocked on an OAM. After <code>qpIPv4Harvest -block_oam_ipv4</code> is finished successfully, this alarm is raised.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm is cleared by <code>qpIPv4Harvest -harvest_oam_only</code> or <code>qpIPv4Harvest -harvest_oam_all</code> .
OID	QPHasBlockedIPv4

Recovery:

Rollback changes in `qpIPv4Harvest -block_oam_ipv4`; Or continue to run `qpIPv4Harvest -harvest_oam_only`.

70039 – QP has blocked IPv4 traffic on all interfaces

Alarm Type	QP
Description	This alarm is raised on each server if IPv4 is blocked on all interfaces. After <code>qpIPv4Harvest -block_all_ipv4</code> is finished successfully, this alarm is raised.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm is cleared by <code>qpIPv4Harvest -harvest_all</code> .
OID	QPHasBlockedIPv4

Recovery:

Rollback changes in `qpIPv4Harvest -block_all_ipv4`; Or continue to run `qpIPv4Harvest -harvest_all`.

70040 – Failure to block IPv4 on the OAM interface

Alarm Type	QP
Description	This alarm is raised when there is a failure to block IPv4 on an OAM interface.
Default Severity	Minor

Instance	N/A
HA Score	Normal
Clearing Action	This alarm will be cleared automatically in 60 minutes. Or it can be cleared once the cluster/site has successfully blocked IPv4 on an OAM interface.
OID	QPFailedToBlockOAMIpv4
Recovery:	
Correct the error conditions and run <code>qpIPv4Harvest -block_oam_ipv4</code> again.	

70041 – Failure to block IPv4 on the all interfaces.

Alarm Type	QP
Description	This alarm is raised when there is a failure to block IPv4 on all interfaces.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm will be cleared automatically in 1 hour. Or it can be cleared once the cluster/site has successfully blocked IPv4 on all interfaces.
OID	QPFailedToBlockAllIpv4
Recovery:	
Correct the error conditions, and run <code>qpIPv4Harvest -block_all_ipv4</code> again.	

70042 – Failure to remove OAM IPv4 addresses from the cluster/site.

Alarm Type	QP
Description	This alarm is raised when there is a failure to remove OAM IPv4 addresses from cluster/site
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm will be cleared automatically in 1 hour. Or it can be cleared once the OAM IPv4 addresses are successfully removed.
OID	QPFailedToRemoveOAMIpv4
Recovery:	
Correct the error conditions and do the harvest again.	

70043 – Failure to remove all IPv4 addresses from the cluster/site

Alarm Type	QP
Description	This alarm is raised when there is a failure to remove all IPv4 addresses from cluster/site.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm will be cleared automatically in 1 hour. Or it can be cleared once all IPv4 addresses are successfully removed.
OID	QPFailedToRemoveAllIpv4

Recovery:

Correct the error conditions and do harvest again.

70044 – Failure to rollback changes for removing IPv4 addresses

Alarm Type	QP
Description	This alarm is raised when there is a failure to rollback changes for removing IPv4 addresses.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm will be cleared automatically in 1 hour. Or it can be cleared once the rollback action finished successfully.
OID	QPFailedToRollbackRecaptureIpv4

Recovery:

Correct the error conditions and do the rollback again.

70050 – QP Timezone change detected

Alarm Type	QP
Description	Time zone has been changed using <code>platacfg</code> . Application needs to be restarted.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears when the application is restarted (<code>qp_procmgr</code> restarted). This is not an auto-clear alarm.

OID QPTimezonechangedetected

Recovery:

If the alarm does not automatically clear within a few seconds or if the alarm is occurring over and over, contact [My Oracle Support \(MOS\)](#).

70500 – System Mixed Version

Alarm Type	QP
Description	There are multiple software versions running in the system because of an upgrade or backout. This alarm is raised when the upgrade director determines that different versions of code are running in the topology. This is expected during an upgrade. It is intended to be a signal that further upgrade activity is required before the system is fully consistent.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	SystemMixedVersion

Recovery:

1. The upgrade director will clear this condition once all servers are running a consistent version.
2. If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

70501 – Cluster Mixed Version

Alarm Type	QP
Description	There are multiple software versions running in a cluster because of an upgrade or backout. Since the cluster is in mixed version, its behavior is likely to be impaired (for example, loss of redundancy/replication). Certain operations may not be possible for the cluster while this alarm is asserted. This alarm is raised when the upgrade director determines that different versions of code are running in the specified cluster. This is expected during an upgrade. It is intended to be a signal that further upgrade activity is required before the cluster is fully consistent.
Default Severity	Minor
Instance	The Comcol ID of the cluster.
HA Score	Normal
Clearing Action	N/A
OID	ClusterMixedVersion

Recovery:

1. The upgrade director will clear this condition once all servers in the cluster are running a consistent version.
2. If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

70502 – Cluster Replication Inhibited

Alarm Type	QP
Description	The upgrade director will inhibit replication to a server if it determines that replication would result in a corrupted database. This can happen if there is an incompatibility between different versions.
Default Severity	Minor
Instance	The Comcol ID of the server. Note: The alarm text will contain the proper host name of the server.
HA Score	Normal
Clearing Action	N/A
OID	ClusterReplicationInhibited

Recovery:

1. Once the server completes the upgrade or backout, the upgrade director will clear the inhibition and the alarm.
2. If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

70503 – Server Forced Standby

Alarm Type	QP
Description	The upgrade director will place a server into forced standby if it is NOT running the same version of software as the active server in the cluster. This alarm signals that the upgrade director has taken this action.
Default Severity	Minor
Instance	The Comcol ID of the server. Note: The alarm text will contain the proper hostname of the server.
HA Score	Normal
Clearing Action	N/A
OID	ServerForcedStandby

Recovery:

1. When the server completes the upgrade or backout, the upgrade director will take the server out of forced standby.
2. If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

70505 – ISO Mismatch

Alarm Type	QP
Description	The server's ISO is not the expected version. This alarm is raised when the upgrade director determines that the 'pending ISO' (the one that would be installed if we attempted an upgrade) is not consistent with what is expected (for example, the wrong version).
Default Severity	Minor
Instance	The Comcol ID of the server. Note: The alarm text will contain the proper host name of the server.
HA Score	Normal
Clearing Action	N/A
OID	ISOMismatch

Recovery:

1. Have the operator remove the offending ISO from `/var/TKLC/log` on the affected machine.
2. If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

70506 – Upgrade Operation Failed

Alarm Type	QP
Description	An action initiated by the upgrade director has failed.
Default Severity	Minor
Instance	The Comcol ID of the server. Note: The alarm text will contain the proper hostname of the server.
HA Score	Normal
Clearing Action	N/A
OID	UpgradeOperationFailed

Recovery:

If the alarm does not automatically clear, contact [My Oracle Support \(MOS\)](#).

70507 – Upgrade In Progress

Alarm Type	QP
Description	An upgrade or backout action on a server is in progress.
Default Severity	Minor

Instance	The Comcol ID of the server. Note: The alarm text will contain the proper host name of the server.
HA Score	Normal
Clearing Action	N/A
OID	UpgradeInProgress

Recovery:

1. Once the upgrade/backout process has completed, the upgrade director will clear this alarm.
2. If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

70508 – Server Is Zombie

Alarm Type	QP
Description	A server has failed an upgrade or backout and now is in an unknown state.
Default Severity	Critical
Instance	The Comcol ID of the server. Note: The alarm text will contain the proper host name of the server.
HA Score	Normal
Clearing Action	N/A
OID	ServerIsZombie

Recovery:

If the alarm does not clear automatically, contact [My Oracle Support \(MOS\)](#).

Policy Server Alarms (71000-79999)

This section provides a list of Policy Server alarms (71000-79999) which are generated by policy devices, such as MPE devices and MRA devices.

71001 – Remote Diversion Not Possible

Alarm Type	PCRF
Description	This alarm occurs when all other associated MRA devices are currently unavailable for remote diversion.
Default Severity	Minor
Instance	N/A

HA Score	Normal
Clearing Action	Auto clear after 7200 seconds.
OID	RemoteDiversionNotPossible

Recovery:

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

71002 – OM Stats Parse Error

Alarm Type	PCRF
Description	OM statistics task could not parse statistics information.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Auto clears after 7200 seconds.
OID	OmStatsParseError

Recovery:

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

71003 – OM Stats Exception Error

Alarm Type	PCRF
Description	OM statistics task could not generate particular statistics due to an exception.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Auto clear after 7200 seconds (120 minutes).
OID	OmStatsExceptionError

Recovery:

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

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	AMConnLost

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

71005 – OM Stats Value Exceed Error

Alarm Type	PCRF
Description	OM statistics value has been truncated to fit the data size.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Auto clears after 7200 seconds.
OID	OmStatsValueExceedError

Recovery:

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

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	DqosDownstreamConnectionClosed

Recovery:

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

71102 – MSC Conn Lost

Alarm Type	PCRF
------------	------

Description	MSC connection 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	MSCConnLost

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

71103 – PCMM Conn Lost

Alarm Type	PCRF
Description	PCMM connection lost. The connection was lost to the specified CMTS or downstream policy server.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Restore the connection to a remote peer.
OID	PCMMConnLost

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

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	DqosAmConnectionClosed

Recovery:

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

71204 – SPC Conn Closed

Alarm Type	PCRF
Description	SPC connection closed.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Connection to a remote peer is restored.
OID	SPCConnClosed

Recovery:

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

71402 – Connectivity Lost

Alarm Type	PCRF
Description	Diameter connection socket is closed.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 7200 seconds or the connection to a Diameter peer is restored.
OID	ConnectivityLost

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

71403 – Connectivity Degraded

Alarm Type	PCRF
-------------------	------

Description	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 or the connection to a Diameter peer is restored.
OID	ConnectivityDegraded

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

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 Settings of the Policy Server tab in the CMP system.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 300 seconds.
OID	DIAMETERNewConnRejected

Recovery:

1. Check the peer configuration and ensure that the peer sees a valid connection with the device.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

71414 – SCTP Path Status Changed

Alarm Type	PCRF
Description	SCTP Path Status Changed. Occurs when an MPE or MRA device 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 (2 hours).
OID	SctpPathStatusChanged

Recovery:

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

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 or clears automatically after 7200 seconds (2 hours).
OID	LdapConnFailed

Recovery:

1. Verify that there is no problem with the LDAP server or the network path used to reach the server.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

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	DHCPUnexpectedEventId

Recovery:

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

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 or clears automatically after 60 seconds.
OID	DHCPUnableToBindEventId

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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	DHCPResponseTimeoutEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

71633 – DHCP 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	DHCPBadRelayAddressEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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	DHCPBadPrimaryAddressEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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	DHCPBadSecondaryAddressEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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 SPRConnectionClosed

Recovery:

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

71685 – MSR DB Not Reachable

Alarm Type	PCRF
Description	Unable to connect to Multimedia Subscriber Repository (MSR) after several attempts.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Connection to MSR is restored.
OID	MSRDBNotReachable

Recovery:

1. Verify that there is no problem with the MSR server or the network path used to reach the server.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

71702 – BRAS Connection Closed

Alarm Type	PCRF
Description	BRAS Connection Closed. The MPE device 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	BrasConnectionClosed

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

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 device.

Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	COPS network element is associated with MPE device.
OID	COPSEUnknownGateway

Recovery:

1. Check the configuration of the network elements in the CMP system. There should be a B-RAS network element for this gateway and that B-RAS must be associated with this MPE device.
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 system must match the provisioned router name on the gateway.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#).

71801 – PCMM No PCEF

Alarm Type	PCRF
Description	This alarm is raised when the MPE cannot find the PCEF. The alarm is disabled by default unless the user sets <code>RC.TrapNoPcefEnabled</code> to true in <code>RCMgr</code> . This update occurs in both the MPE-R and MPE-S. The <code>SubId</code> in the alarm details is actually CMTSIP if the MPE uses CMTSIP to find PCEF when it receives PCMM requests. The PCMM requests may be <code>GateSet/GateInfo/GateDelete</code> .
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 60 seconds.
OID	PCMMNoPCEF

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

71805 – PCMM Non Connection 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	PCMMNonConnectionPCEF

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

72198 – SMSR SMSC Switched to Primary

Alarm Type	PCRF
Description	Switched to primary Short Message Service Center (SMSC). Switched from Secondary to Primary SMSC.
Default Severity	Minor
Instance	SMSC address
HA Score	Normal
Clearing Action	This alarm automatically clears after 60 minutes (3600 seconds).
OID	SMSRSMSCSwitchedToPrimary

Recovery:

No action necessary.

72199 – SMSR SMSC Switched to Secondary

Alarm Type	PCRF
Description	Switched to Secondary Short Message Service Center (SMSC). Switched from Primary to Secondary SMSC.
Default Severity	Minor
Instance	SMSC Address
HA Score	Normal
Clearing Action	This alarm automatically clears after 60 minutes (3600 seconds).
OID	SMSRSMSCSwitchedToSecondary

Recovery:

No action necessary.

72210 – PCMM Reached Max Gates Event ID

Alarm Type	PCRF
Description	PCMM Reached Maximum Gates. A subscriber at IP address <i>ip-addr</i> 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	PCMMReachedMaxGatesEventId

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

72211 – PCMM Reached Max GPI Event ID

Alarm Type	PCRF
Description	PCMM Reached Maximum GPI. A subscriber at IP address <i>ip-addr</i> 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	PCMMReachedMaxGPIEventId

Recovery:

1. This subscriber address is exceeding the capacity; attention is required.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

72501 – SCE Connection Lost

Alarm Type	PCRF
Description	Service Control Engine (SCE) Connection is lost.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Connection to SCE is restored.
OID	SCEConnectionLost

Recovery:

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

72549 – SMSR Queue Full

Alarm Type	PCRF
Description	Short Message Service Relay (SMSR) internal queue is full: notification internal queue has reached capacity. Messages will be rejected until the queue space becomes available.
Default Severity	Minor
Instance	SMSR queue
HA Score	Normal
Clearing Action	Available capacity is restored and queue begins to accept new messages or automatically clears after 60 minutes (3600 seconds).
OID	SMSRQueueFull

Recovery:

Check configuration and availability of the destination service to ensure there are no connections problems and that the network path from the MPE device to the element (host/port/resource location) is operational.

72559 – SMSR SMSC Connection Closed

Alarm Type	PCRF
Description	SMSC connection closed.
Default Severity	Minor
Instance	SMSC address
HA Score	Normal
Clearing Action	This alarm automatically clears after 60 minutes (3600 seconds) or when the SMSC connection is restored.
OID	SMSRSMSCConnectionClosed

Recovery:

No action necessary.

72565 – SMSR SMTP Connection Closed

Alarm Type	PCRF
Description	Simple Mail Transfer Protocol (SMTP) connection closed. SMTP connection has been closed to MTA <i>{IP Address}</i> .
Default Severity	Minor
Instance	<i>{host name of MTA}</i>
HA Score	Normal

Clearing Action This alarm automatically clears after 60 minutes (3600 seconds) or when the SMTP connection is restored.

OID SMSRSMTPConnectionClosed

Recovery:

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

72575 – SMSR HTTP Connection Closed

Alarm Type	PCRF
Description	The connection to a configured Policy Notification destination was lost.
Default Severity	Minor
Instance	Destination Name
HA Score	Normal
Clearing Action	Auto clears after 60 minutes (3600 seconds) or when HTTP connection is restored.
OID	SMSRHTTPConnectionClosed

Recovery:

1. Check configuration, including URL, and availability of the destination service.
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 (host/port/resource location) is operational.
4. If the problem persists, contact [My Oracle Support \(MOS\)](#).

72703 – RADIUS Server Failed

Alarm Type	PCRF
Description	RADIUS server start failed.
Default Severity	Minor
Instance	N/A
HA Score	N/A
Clearing Action	N/A
OID	RADIUSServerFailed

Recovery:

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

72706 - RADIUS Server Corrupt Auth

Alarm Type	PCRF
Description	RADIUS authenticator is corrupted.
Severity	Minor
Instance	N/A
HA Score	N/A
Clearing Action	N/A
OID	RADIUServerCorrupAuth

Recovery:

Check the connectivity and configuration of the RADIUS server.

72904 – Diameter Too Busy

Alarm Type	PCRF
Description	System has entered 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	DiameterTooBusy

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

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	RadiusTooBusy

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support \(MOS\)](#).

74000 – Policy Server 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 (60 minutes).
OID	PolicyServerCriticalAlarm

Recovery:

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

74001 – Policy Server 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 (60 minutes).
OID	PolicyServerMajorAlarm

Recovery:

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

74002 – Policy Server 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 (60 minutes).

OID PolicyServerMinorAlarm

Recovery:

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

74020 – Stats Files Generator Delete Expire Files

Alarm Type	PCRF
Description	Delete expire files. Stats Files Generator Task has removed some files which were not synchronized to remote servers (<i>{external system IP}</i> , <i>{external system IP}</i> , etc).
Default Severity	Major
Instance	Stats files generator
HA Score	Normal
Clearing Action	The alarm is automatically cleared after 300 seconds (5 minutes).
OID	StatsFilesGeneratorDeleteExpireFiles

Recovery:

Check all enabled Stats Files Synchronization tasks status in the DC (Data Collection) tasks of CMP system and ensure they are configured successfully.

74021 – Files Synchronization Failure

Alarm Type	PCRF
Description	Files synchronization failure. Files Synchronization <i>#{num}</i> task failed to synchronize local to remote server (<i>{external system Host Name/IP}</i>) after retry <i>{num}</i> times, where: <ul style="list-style-type: none"> <i>{num}</i> is task # <i>{num}</i> is retry times (1 to 5) <i>{external system Host Name/IP}</i> is the user-defined remote server's IP address to which files are synchronized
Default Severity	Minor
Instance	Stats files synchronization
HA Score	Normal
Clearing Action	Auto clear 300 seconds
OID	FilesSynchronizationFailure

Recovery:

1. Check the network status of the remote server which you configured in the Stats Files Synchronization task.
2. Ensure remote server supports SSH protocol and you configured the user name and password correctly.

74022 - Files Uploading Failure

Alarm Type	PCRF
Description	PM Statistics Files Uploading Task failed to upload local statistics files to FTP server <i>FTP server Host Name/IP</i> after retry <i>number</i> times.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	This alarm automatically clears after 5 minutes (300 seconds).
OID	FilesUploadingFailureNotify

Recovery:

1. Fix network problems or verify FTP configuration information, which is defined in the scheduler task of the CMP system.
2. If the issue does not resolve, contact [My Oracle Support \(MOS\)](#).

74102 - CMTS Subnet Overlapped

Alarm Type	
Description	Overlapped subnets are present on the CMTS.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Auto clears when task runs again.
OID	CmtsSubnetOverlapped

Recovery:

1. Go to Schedule Tasks Administration with menu item **System Administration > Scheduled Tasks**.
2. Open Subnet Overlap Detector Task hyperlink.
3. Open Subnet Overlapping Report by clicking 'details' hyperlink in Exit Status Message.
4. Refer to Subnet Overlap Report for overlapped subnets of CMTS detail information.
5. Reconfigure the subnets of CMTS to resolve the overlap.
6. Run the Subnet Overlap Detector task again.
7. If the issue still exists, repeat the previous steps.

74103 - NES Without CMTS IP

Alarm Type	
Description	This alarm is raised when Routing by CMTS IP is enabled and Network Elements exist without CMTS IP addresses assigned.

Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm automatically clears after 30 seconds.
OID	NeWithoutCmtsIp

Recovery:

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

74602 - 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	Major
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears when HA recovers or clears automatically after 30 minutes (1800 seconds). When HA recovers there will be only one Active server in a cluster.
OID	QPMultipleActiveInClusterFailure

Recovery:

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. If the problem persists, contact [My Oracle Support \(MOS\)](#).

74603 - Max Primary Cluster Failure Threshold

Alarm Type	QP
Description	The number of failed MPE pairs reaches the threshold of <i>configured threshold value</i> at <i>site name</i> .
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 <i>max primary site failure threshold</i> at <i>site</i> , or clears automatically after 30 minutes (1800 seconds).
OID	QPMMaxMPEPrimaryClusterFailure

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 does not clear automatically, contact [My Oracle Support \(MOS\)](#).

74604 - MPE 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 (1800 seconds).
OID	QPMPEClusterOfflineFailure

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 does not clear automatically, contact [My Oracle Support \(MOS\)](#).

74605 - Subscriber Trace Backup Failure

Alarm Type	QP
Description	The script responsible for backing up the subscriber trace log has failed.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	
OID	SubscriberTraceBackupFailure

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 does not clear automatically, contact [My Oracle Support \(MOS\)](#).

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	PolicyLoadingLibraryFailed

Recovery:

1. Perform a reapply config from the CMP system to reload the library.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

77904 - BOD PCMM Too Busy

Alarm Type	PCRF
Description	BOD PCMM load shedding set a busy state.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 30 seconds.
OID	BODPCMMTooBusy

Recovery:

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

77905 - BOD DIAMETER Too Busy

Alarm Type	PCRF
Description	BOD DIAMETER Too Busy
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 30 seconds.
OID	BODDiameterTooBusy

Recovery:

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

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 automatically clears in 60 minutes (3600 seconds).
OID	ADSConnectionLost

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

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 server when a policy change is made or a Reapply Configuration is performed. It can be raised by the standby server during startup if it was unable to get the policy jar file from the active server 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 automatically clear in 60 minutes (3600 seconds).
OID	RsyncFailed

Recovery:

1. This alarm can be ignored during a mixed version upgrade (for example, 7.5/7.6 to 9.1) and when rebooting both servers on the MPE device.
2. If the alarm is seen on the MRA device, 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 [My Oracle Support \(MOS\)](#).

79002 - Sess DB Size Reached Threshold

Alarm Type	PCRF
Description	Total session database size reached maximum threshold percentage of planned session database size.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Total session database size goes below minimum threshold percentage of planned session database size.
OID	SessDBSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the customer's expectation.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

79003 - Avg Sess Size Reached Threshold

Alarm Type	PCRF
Description	Average session size exceeded the projected size.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 60 minutes (3600 seconds).
OID	AvgSessSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the customer's expectation.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

79004 - Bind DB Size Reached Threshold

Alarm Type	PCRF
-------------------	------

Description	Total binding database size reached maximum threshold percentage of planned binding database size.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Total binding database size goes below minimum threshold percentage of planned binding database size or clears automatically after 60 minutes (3600 seconds).
OID	BindDBSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the customer's expectation.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

79005 - Avg Bind Size Exceeded

Alarm Type	PCRF
Description	Average binding size exceeded the projected size.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 60 minutes (3600 seconds).
OID	vgBindSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the customer's expectation.
2. If the problem persists, contact [My Oracle Support \(MOS\)](#).

79105 - Mediation SOAP Too Busy

Alarm Type	PCRF
Description	Mediation Server SOAP provisioning interface reaches busy state; load shedding begins.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	MediationSOAPTTooBusy

Recovery:

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

79106 - SPR Connection Failed

Alarm Type	PCRF
Description	Created connection to SPR failed.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	SPRConnectionFailed

Recovery:

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

79107 - Mediation Disk Quota Exceed

Alarm Type	PCRF
Description	Sync directory disk quota exceeded.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	MSDiskQuotaExceed

Recovery:

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

79108 - Mediation Disk No Space

Alarm Type	PCRF
Description	No space left on device.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	MSDiskNoSpace

Recovery:

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

79109 - SPR License Limit

Alarm Type	PCRF
Description	Achieve 80% maximum number of users in SPR.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	SPRLicenseLimit

Recovery:

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

79110 - Stats File Upload Fail

Alarm Type	PCRF
Description	1. SMS Notification Statistics Uploading Task failed to upload local stat files to FTP server (<FTP server Host Name/IP>) after retry <N> times, where FTP server Host Name/IP: FTP server in the configured task and N: 0-5 retry times.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	300
OID	StatsFileUploadFailure

Recovery:

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

79120 - Batch Folder Disk Quota Exceeds

Alarm Type	PCRF
Description	The batch folder disk quota has been exceeded.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	BatchDiskQuotaExceeds

Recovery:

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

79995 - X1 Connection Lost

Alarm Type	PCRF
Description	The X1 Connection between the Mediation Function and Policy Server is Lost.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 7200 seconds.
OID	X1ConnectionLost

Recovery:

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

79996 - X2 Connection Lost

Alarm Type	PCRF
Description	X2 Connection between the Policy Server and Mediation Function is Lost.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 7200 seconds.
OID	X2ConnectionLost

Recovery:

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

Policy Server Events (80000-89999)

This section provides a list of Policy Server events (80000-89999) which are generated by policy devices, such as MPE devices and MRA devices.

80001 - 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 <code>qp-procmgr</code> as <code>qp-procmgr</code> shuts down.
OID	QPDDBStateChange

Recovery:

No action required.

80002 - MySQL Relay Log Dropped

Alarm Type	QP
Description	A portion of the MySQL relay log was dropped as the secondary server was shutting down. This event is raised when a secondary server times out while trying to apply its relay log during a secondary stop. The server may not be hurt, but there may be after effects. This event is raised to trigger a debug for possible after effects.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	QPMysqlRelayLogDropped

Recovery:

Debug the system for possible after effects caused by the timeout.

80003 - QP MySQL DB Level

Alarm Type	QP
Description	The ranking of secondaries when the primary database is outdated. If the primary database is outdated, the server raises this event once per minute. The server will rank the secondaries, from best to worst, based on their database level.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	QPMysqlDBLevel

Recovery:

Use the information of this event to help resolve an outdated primary 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	BindingReleaseTask

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	PolicyInfoEvent

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	ApplicationIsReady

Recovery:

No action required.

86100 - CMP User Login

Alarm Type	PCRF
Description	CMP user login was successful.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserLogin

Recovery:

No action required.

86101 - CMP User Login Failed

Alarm Type	PCRF
Description	CMP user login failed.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserLoginFailed

Recovery:

No action required.

86102 - CMP User Logout

Alarm Type	PCRF
Description	CMP User performed logout.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserLogout

Recovery:

No action required.

86200 - CMP User Promoted Server

Alarm Type	PCRF
Description	CMP user promoted server.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserPromotedServer

Recovery:

No action required.

86201 - CMP User Demoted Server

Alarm Type	PCRF
Description	CMP user demoted server.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserDemotedServer

Recovery:

No action required.

86300 - Sh Enable Failed

Alarm Type	PCRF
Description	Enable Sh Connection failed. The CMP server performed a global operation to enable Sh on all MPE devices and it failed on the specified MPE.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPSHConEnableFailed

Recovery:

The operation can be retried. If repeated attempts fail, there may be other management issues with the associated MPE devices 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 devices and it failed on the specified MPE.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPSHConDisableFailed

Recovery:

The operation can be retried. If repeated attempts fail, there may be other management issues with the associated MPE devices and connectivity to those devices should be verified.

86303 - NW-CMP Apply Failed

Alarm Type	PCRF
Description	NW-CMP failed to apply settings to S-CMP.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	NWCMPApplyFailed

Recovery:

The alarm on the NW-CMP will be cleared once the NW-CMP successfully applies the configuration to the S-CMP.

86304 - S-CMP Unreachable

Alarm Type	PCRF
Description	The S-CMP is offline or unreachable by the NW-CMP. This alarm will be raised on the NW-CMP.
Default Severity	Major
Instance	N/A

HA Score	Normal
Clearing Action	N/A
OID	SCMPUNREACHABLE

Recovery:

This alarm will be cleared once the S-CMP is reachable.

86305 - S-CMP Split Brain

Alarm Type	PCRF
Description	When a geo-redundant S-CMP is in split brain (that is, both sites are reporting as Primary), an alarm is raised on NW-CMP.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	SCMPSplitBrain

Recovery:

This alarm will be cleared automatically when the split brain on the S-CMP is gone.

86306 - CMP Apply Failed

Alarm Type	PCRF
Description	When a CMP system failed to apply settings to any MRA or MPE device, this alarm is raised on this S-CMP.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPApplyFailed

Recovery:

This alarm will be cleared automatically when the next applying to that MRA or MPE device is successful.

86307 - S-CMP Sync Fails

Alarm Type	PCRF
-------------------	------

Description	If the connection between the NW-CMP and the S-CMP is broken and the synchronization fails, an alarm will be raised in S-CMP.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	SCMPSYNCFAILS

Recovery:

The alarm will be cleared once the synchronization is successful in the next cycle.

86308 - NCMP Ref Obj Miss

Alarm Type	PCRF
Description	The top level object is missing in NW-CMP but is referred by S-CMP server. This alarm will be raised in the NW-CMP server.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	NCMPReferdObjMiss

Recovery:

This alarm will be cleared once there is no referred but missing top level object.

Chapter 6

Obtaining SNMP Status and Statistics

Topics:

- *Obtaining CMTS and DPS Connection Status.....163*
- *Obtaining Rx and Diameter AF Operation Measurement Statistics.....163*
- *Obtaining PCMM Operation Measurement Statistics.....165*

This chapter describes how to obtain status and statistical information from a cable-mode Policy Management system using the SNMP interface.

Obtaining CMTS and DPS Connection Status

Using an SNMP GetNext request, you can obtain connection status information from the following Tables:

- `cmtsConnTable` for cable modem termination systems (CMTSs)
- `dpsConnTable` for downstream policy servers (DPSs)

The following information is reported for each network element of both kinds of devices:

- ID
- Host Name
- Connection Type
- Connection Status
- Last Connection Time
- Last Disconnection Time
- Collection Time Stamp

Counters are updated every thirty seconds.

You can obtain this data using a variety of SNMP applications. The example shown in [Figure 4: Sample CMTS And DPS Connection Table Statistics](#) uses `snmpwalk`.

```
# snmpwalk -c public 10.24.19.54 -m TKLC-APP-MIB cmtsConnTable
TKLC-APP-MIB::cmtsHostName..."f" = STRING: 10.0.7.102
TKLC-APP-MIB::cmtsID..."f" = STRING: cmts
TKLC-APP-MIB::cmtsConnStatus..."f" = INTEGER: disconnected(2)
TKLC-APP-MIB::cmtsLastConnTime..."f" = Counter64: 0
TKLC-APP-MIB::cmtsLastDisconnTime..."f" = Counter64: 0
TKLC-APP-MIB::cmtsCollectTime..."f" = Counter64: 1275496585399

# snmpwalk -c public 10.24.19.54 -m TKLC-APP-MIB dpsConnTable
TKLC-APP-MIB::dpsHostName..."d".pcmm = STRING: 10.0.10.100
TKLC-APP-MIB::dpsConnType..."d".pcmm = INTEGER: pcmm(1)
TKLC-APP-MIB::dpsID..."d".pcmm = STRING: mpeadam
TKLC-APP-MIB::dpsConnStatus..."d".pcmm = INTEGER: connected(1)
TKLC-APP-MIB::dpsLastConnTime..."d".pcmm = Counter64: 1275417944367
TKLC-APP-MIB::dpsLastDisconnTime..."d".pcmm = Counter64: 1275417899375
TKLC-APP-MIB::dpsCollectTime..."d".pcmm = Counter64: 1275496622064
#
```

Figure 4: Sample CMTS And DPS Connection Table Statistics

Obtaining Rx and Diameter AF Operation Measurement Statistics

Using an SNMP GetNext request, you can obtain operation measurement (OM) statistics from `diameterOMStats` for the Rx and Diameter protocols. The following OM counters are reported:

- AAR Initial messages received

- AAR Initial messages sent
- AAR Modification messages received
- AAR Modification messages sent
- AAR Received messages
- AAR Received Success messages
- AAR Received Failure messages
- AAR Sent messages
- AAR Sent Success messages
- AAR Sent Failure messages
- STR Received messages
- STR Sent messages
- STA Received Success messages
- STA Received Failure messages
- STA Sent Success messages
- STA Sent Failure messages
- ASR Received messages
- ASR Sent messages
- ASA Received Success messages
- ASA Received Failure messages
- ASA Sent Success messages
- ASA Sent Failure messages
- RAR Received messages
- RAR Sent messages
- RAA Received Success messages
- RAA Received Failure messages
- RAA Sent Success messages
- RAA Sent Failure messages
- Collection time
- Reset time
- Rx-PCMM messages timeout counter

Counter values are absolute values. Counters are updated every five minutes.

You can obtain OM statistics using a variety of SNMP applications. The example shown in [Figure 5: Sample Rx/Diameter OM Statistics](#) uses `snmpwalk`.

```
# snmpwalk -c public 10.24.19.54 -m TKLC-APP-MIB diameterOMStats
TKLC-APP-MIB::diameterOMAARRecv.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAARSent.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAAARcvSuccess.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAAARcvFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMAAASentSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMAAASentFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMSTRRecv.0 = Counter32: 0
TKLC-APP-MIB::diameterOMSTRSent.0 = Counter32: 0
TKLC-APP-MIB::diameterOMSTARcvSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMSTARcvFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMSTASentSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMSTASentFailure.0 = Counter32:
```

```

TKLC-APP-MIB::diameterOMASRRecv.0 = Counter32: 0
TKLC-APP-MIB::diameterOMASRSent.0 = Counter32: 0
TKLC-APP-MIB::diameterOMASARcvSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMASARcvFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMASASentSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMASASentFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMRARRecv.0 = Counter32: 0
TKLC-APP-MIB::diameterOMRARSent.0 = Counter32: 0
TKLC-APP-MIB::diameterOMRAARcvSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMRAARcvFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMRAASentSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMRAASentFailure.0 = Counter32:
TKLC-APP-MIB::diameterOMCollectTime.0 = Counter64: 0
TKLC-APP-MIB::diameterOMResetTime.0 = Counter64: 0
TKLC-APP-MIB::diameterOMAARInitRecv.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAARInitSent.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAARModRecv.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAARModSent.0 = Counter32: 0
TKLC-APP-MIB::diameterOMRxPcmmTimeout.0 = Counter32: 0
#

```

Figure 5: Sample Rx/Diameter OM Statistics

Obtaining PCMM Operation Measurement Statistics

Using an SNMP GetNext request, you can obtain operation measurement (OM) statistics for the PacketCable MultiMedia (PCMM) protocol.

OM statistics are reported from

- northBoundPcmmOMStats for northbound traffic between application managers (AMs) and MPE devices
- southBoundPcmmCmtsOMStats for southbound traffic between MPE devices and CMTSs
- southBoundPcmmDpsOMStats for southbound traffic between MPE devices and DPSs

The following OM counters are reported:

- Gate Set messages
- Gate Set Acknowledgment messages
- Gate Set Error messages
- Gate Delete messages
- Gate Delete Acknowledgment messages
- Gate Delete Error messages
- Gate Info messages
- Gate Info Acknowledgment messages
- Gate Info Error messages
- Gate Report messages
- Gate Report Drop messages
- Collection time
- Reset time

Counters are updated every five minutes.

You can obtain PCMM OM statistics using a variety of SNMP applications. The example shown in [Figure 6: Sample PCMM Northbound And Southbound OM Statistics](#) uses `snmpwalk`.

```
# snmpwalk -c public 10.24.19.54 -m TKLC-APP-MIB northBoundPcmmOMStats
TKLC-APP-MIB::northBoundPcmmOMGateSet.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateSetAck.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateSetErr.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateInfo.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateInfoAck.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateInfoErr.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateDelete.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateDeleteAck.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateDeleteErr.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateReport.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMGateReportDrop.0 = Counter32: 0
TKLC-APP-MIB::northBoundPcmmOMCollectTime.0 = Counter64: 0
TKLC-APP-MIB::northBoundPcmmOMResetTime.0 = Counter64: 0

# snmpwalk -c public 10.24.19.54 -m TKLC-APP-MIB southBoundPcmmCmtsOMStats
TKLC-APP-MIB::southBoundPcmmCmtsOMGateSet.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateSetAck.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateSetErr.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateInfo.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateInfoAck.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateInfoErr.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateDelete.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateDeleteAck.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateDeleteErr.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateReport.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMGateReportDrop.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmCmtsOMCollectTime.0 = Counter64: 1275496500897
TKLC-APP-MIB::southBoundPcmmCmtsOMResetTime.0 = Counter64: 0

# snmpwalk -c public 10.24.19.54 -m TKLC-APP-MIB southBoundPcmmDpsOMStats
TKLC-APP-MIB::southBoundPcmmDpsOMGateSet.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateSetAck.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateSetErr.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateInfo.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateInfoAck.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateInfoErr.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateDelete.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateDeleteAck.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateDeleteErr.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateReport.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMGateReportDrop.0 = Counter32: 0
TKLC-APP-MIB::southBoundPcmmDpsOMCollectTime.0 = Counter64: 1275496800903
TKLC-APP-MIB::southBoundPcmmDpsOMResetTime.0 = Counter64: 0
#
```

Figure 6: Sample PCMM Northbound And Southbound OM Statistics

A

AM	<p>Application Manager</p> <p>A server within a network that is responsible for establishing and managing subscriber sessions associated with a specific application.</p>
ASA	<p>Analysis Service Application</p>

B

B-RAS	<p>Broadband Remote Access Server</p> <p>Routes traffic to and from broadband remote access devices such as DSL multiplexers. The locations where policy management and DQoS functions occur. Also see BNG.</p>
-------	---

C

CMOS	<p>Complementary Metal Oxide Semiconductor</p> <p>CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.</p>
CMP	<p>Configuration Management Platform</p> <p>A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple</p>

C

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.

Equipment used by cable companies to provide high speed data services to cable subscribers.

COPS-PR

Common open policy servers protocol for support of policy provisioning

D

DB

Database

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

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.

F

FABR

Full Address Based Resolution

F

Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.

FIPS

Federal Information Processing Standard

Full Address Based Resolution

See FABR.

G

GUI

Graphical User Interface
The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA

High Availability
High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

HIDS

Host Intrusion Detection System

HP

Hewlett-Packard

I

IP

Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used

I

on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

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.

MTA

Mail Transfer Agent (or Message Transfer Agent)

Email server software that transfers electronic mail messages from one computer to another.

Multimedia Policy Engine

See MPE.

Multiprotocol Routing Agent

See MRA.

N

N

NTP	Network Time Protocol
NTP daemon	Network Time Protocol daemon – NTP process that runs in the background.
NW-CMP	<p>Network Configuration Management Platform</p> <p>The NW-CMP server configures Network tier objects. Examples of Network tier objects are policies, network elements, and configuration templates.</p>

O

OID	<p>Object Identifier</p> <p>An identifier for a managed object in a Management Information Base (MIB) hierarchy. This can be depicted as a tree, the levels of which are assigned by different organizations. Top level MIB OIDs belong to different standard organizations. Vendors define private branches that include managed objects for their own products.</p>
-----	---

OM	Operational Measurement
----	-------------------------

P

PCMM	PacketCable MultiMedia
PDU	Protocol Data Unit
Perl	An object-oriented, event-driven programming language.

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

RBAR Range Based Address Resolution
A DSR enhanced routing application which allows you to route Diameter end-to-end transactions based on Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges.

S

S-CMP System Configuration Management Platform
The S-CMP servers configure System tier objects. System tier objects are MPE and MRA devices.

Simple Network Management Protocol See SNMP.

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

S

(MIB). The SNMP protocol arranges managed objects into groups.

SOAP

Simple Object Access Protocol

SPC

Service Provisioning over COPS (Common Open Policy Service protocol)

STR

Send_to_Resource AIN message
Session Termination Request (Rx Diameter command)

T

TCP

Transmission Control Protocol

A connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner.

U

UDP

User Datagram Protocol

V

VIP

Virtual IP Address

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.