Oracle® Communications Policy Management

SNMP User's Guide

Release 12.2

E66969 Revision 01

November 2016

ORACLE

Oracle Communications Policy Management SNMP User's Guide, Release 12.2

Table of Contents

List of Figures

List of Tables

Chapter 1

About This Guide

Topics:

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

Icon	Description
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Specifications

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

Locate Product Documentation on the Oracle Help Center Site

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

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

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Chapter 2

Overview

Topics:

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:

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*).

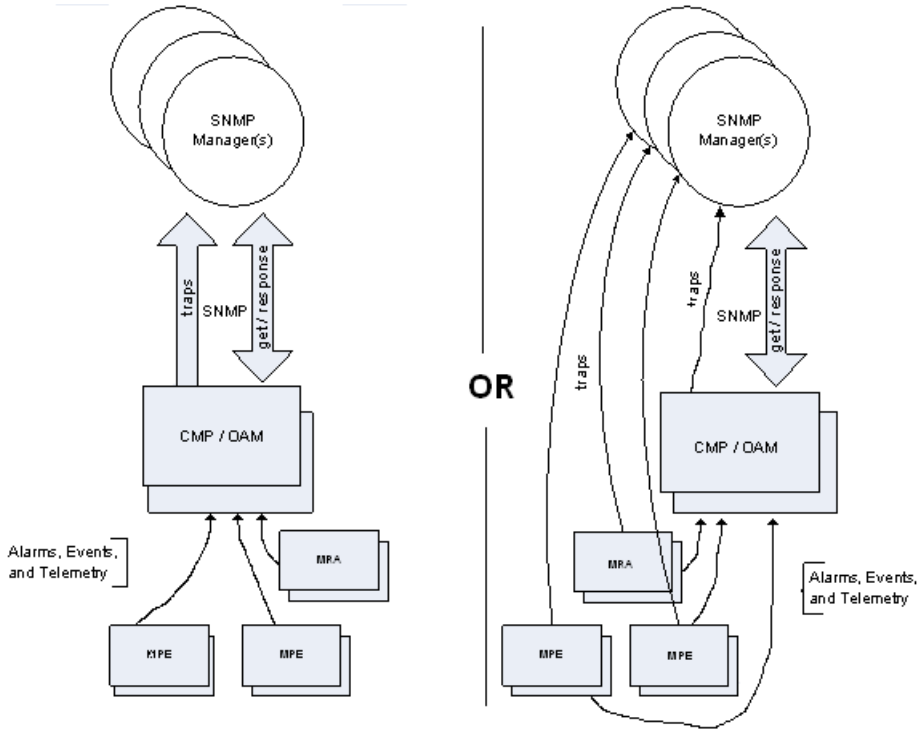

Figure 1: SNMP Configuration

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 CMP 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 using a user name with administrator privileges.
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 SNMP Manager, enter a valid host name or an IPv4IPv4/IPv6 address.

   The **Hostname/IP Address** field is required for an SNMP Manager to receive traps and send SNMP requests. The field has 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).

   By default, these fields are blank.

   Note: The IPv6 address is not supported.

5. (Optional) You can configure a port for each SNMP Manager by entering a port value between 1 and 65535 in the **Port** field. If left blank, the default value is 162.
6. From the **Enabled Versions** list, select one of the following versions

   - **SNMPv2c**
   - **SNMPv3**
   - **SNMPv2c and SNMPv3** (default)

7. If you selected **SNMPv2c** or **SNMPv2c and SNMPv3** from the **Enabled Versions** list, configure the following:

   a) **Traps Enabled** — Specifies whether sending SNMPv2 traps is enabled. The default is enabled.

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

b) **Traps from individual Servers** — Specifies whether sending SNMPv2 traps from individual servers is enabled. If disabled, SNMPv2 traps are only sent from the active CMP system only. The default is disabled.

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

c) **SNMPv2c Community Name** — Enter 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`**.

8. If you selected **SNMPv3** or **SNMPv2c and SNMPv3** from the **Enabled Versions** list, configure the following:

a) **SNMPv3 Engine ID** — Enter an Engine ID for SNMPv3. The Engine ID can be 10 to 64 digits long and must use only hexadecimal digits (0-9 and a-f). The default is no value (null).

b) **SNMPv3 Security Level** — Select the level of 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.

c) **SNMPv3 Authentication Type** — Select an SNMPv3 authentication protocol from the list:

- **SHA-1** — Use Secure Hash Algorithm authentication.
- **MD5** (default) — Use Message Digest authentication.

d) **SNMPv3 Privacy Type** — Select an SNMPv3 privacy protocol from the list:

- **AES** (default) — Use Advanced Encryption Standard privacy.
- **DES** — Use Data Encryption Standard privacy.

e) **SNMPv3 Username** — Enter a user name. The user name can contain 0 to 32 characters and must only contain alphanumeric characters. The default is **`TekSNMPUser`**.

f) **SNMPv3 Password** — Enter an authentication password. The password must contain between 8 and 64 characters and can include any character. The default is **`snmpv3password`**.

Note: The SNMPv3 password is also used for `msgPrivacyParameters`.

9. 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.

10. 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.

11. 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`**.

12. 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 value is no value (null).

13. 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.

14. 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.

15. 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.

16. 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`**.

17. 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`**.

18. Click **Save**.

The SNMP settings for the network are configured.

Chapter 4

Supported MIBs

Topics:

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 `Table` objects by adding a '.0' (dot-zero) extension to their names. (If the '.0' 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 '.' (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:

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 31000-32800.

31000 - S/W fault

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

OID:	comcolSwFaultNotify

Recovery:

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

31001 - S/W status

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

Recovery:

No action required.

31002 - Process watchdog failure

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

Recovery:

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

31003 - Tab thread watchdog failure

Alarm Group:	SW
Description:	Tab thread watchdog timed out
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

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

31100 - Database replication fault

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

Recovery:

1. Export event history for the given server and inetsync task.
2. It is recommended to contact *My Oracle Support (MOS)*.

31101 - Database replication to slave failure

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

Recovery:

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

31102 - Database replication from master failure

Alarm Group:	REPL

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

Recovery:

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

31103 - DB Replication update fault

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

Recovery:

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

31104 - DB Replication latency over threshold

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

Recovery:

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

31105 - Database merge fault

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

Recovery:

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

31106 - Database merge to parent failure

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

Recovery:

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

31107 - Database merge from child failure

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

Recovery:

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

31108 - Database merge latency over threshold

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

Recovery:

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

31109 - Topology config error

Alarm Group:	DB
Description:	Topology is configured incorrectly
Severity:	Minor

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

Recovery:

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

31110 - Database audit fault

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

Recovery:

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

31111 - Database merge audit in progress

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

Recovery:

No action required.

31112 - DB replication update log transfer timed out

Alarm Group:	REPL
Description:	DB Replicated data may not have transferred in the time allotted.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	30
OID:	comcolDbRepUpLogTransTimeoutNotify

Recovery:

1. No action required.
2. It is recommended to contact *My Oracle Support (MOS)* if this occurs frequently.

31113 - DB replication manually disabled

Alarm Group:	REPL
Description:	DB Replication Manually Disabled
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolDbReplicationManuallyDisabledNotify

Recovery:

No action required.

31114 - DB replication over SOAP has failed

Alarm Group:	REPL
Description:	Database replication of configuration data via SOAP has failed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	3600
OID:	comcolDbReplicationSoapFaultNotify

Recovery:

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

31115 - Database service fault

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

Recovery:

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

31116 - Excessive shared memory

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

Recovery:

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

31117 - Low disk free

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

Recovery:

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

31118 - Database disk store fault

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

Recovery:

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

31119 - Database updatelog overrun

Alarm Group:	DB
Description:	The Database update log was overrun increasing risk of data loss
Severity:	Minor

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

Recovery:

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

31120 - Database updatelog write fault

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

Recovery:

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

31121 - Low disk free early warning

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

Recovery:

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

31122 - Excessive shared memory early warning

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

Recovery:

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

31123 - Database replication audit command complete

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

Recovery:

No action required.

31124 - ADIC error

Alarm Group:	REPL
Description:	An ADIC detected errors
Severity:	Minor

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

Recovery:

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

31125 - Database durability degraded

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

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

31126 - Audit blocked

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

Recovery:

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

31127 - DB Replication Audit Complete

Alarm Group:	REPL
Description:	DB replication audit completed
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolDbRepAuditCompleteNotify

Recovery:

No action required.

31128 - ADIC Found Error

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

Recovery:

1. This alarm indicates a data integrity error was found by the background database audit mechanism, and there is no automatic recovery.
2. It is recommended to contact *My Oracle Support (MOS)*.

31129 - ADIC Found Minor Issue

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

Auto Clear Seconds:	14400
OID:	comcolDbADICWarn

Recovery:

No action required.

31130 - Network health warning

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

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

31131 - DB Ousted Throttle Behind

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

Recovery:

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

31140 - Database perl fault

Alarm Group:	SW

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

Recovery:

1. This alarm indicates an error has occurred within a Perl script, but the system has recovered.
2. If the alarm occurs repeatedly, it is recommended to contact *My Oracle Support (MOS)*.

31145 - Database SQL fault

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

Recovery:

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

31146 - DB mastership fault

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

Recovery:

1. Export event history for the given server.
2. It is recommended to contact *My Oracle Support (MOS)*.

31147 - DB upsynclog overrun

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

Recovery:

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

31148 - DB lock error detected

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

Recovery:

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

31200 - Process management fault

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

Recovery:

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

31201 - Process not running

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

Recovery:

1. This alarm indicates that the managed process exited unexpectedly due to a memory fault, but the process was automatically restarted.
2. It is recommended to collect savelogs and contact *My Oracle Support (MOS)*.

31202 - Unkillable zombie process

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

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

Recovery:

1. This alarm indicates managed process exited unexpectedly and was unable to be restarted automatically.
2. It is recommended to collect savelogs and contact *My Oracle Support (MOS)*.

31206 - Process mgmt monitoring fault

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

Recovery:

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

31207 - Process resource monitoring fault

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

Recovery:

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

31208 - IP port server fault

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

Recovery:

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

31209 - Hostname lookup failed

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

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

31213 - Process scheduler fault

Alarm Group:	SW
Description:	The process scheduler (ProcSched/runat) is impaired by a s/w fault
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

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

31214 - Scheduled process fault

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

Recovery:

1. This alarm indicates that a managed process exited unexpectedly due to a memory fault, but the system has recovered.
2. It is recommended to contact *My Oracle Support (MOS)*.

31215 - Process resources exceeded

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

Recovery:

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

31216 - SysMetric configuration error

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

Recovery:

1. This alarm indicates a system metric is configured incorrectly.
2. It is recommended to contact *My Oracle Support (MOS)*.

31220 - HA configuration monitor fault

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

Recovery:

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

31221 - HA alarm monitor fault

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

Recovery:

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

31222 - HA not configured

Alarm Group:	HA
Description:	High availability is disabled due to system configuration
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	300
OID:	comcolHaNotConfiguredNotify

Recovery:

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

31223 - HA Heartbeat transmit failure

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

Recovery:

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

31224 - HA configuration error

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

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

Recovery:

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

31225 - HA service start failure

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

Recovery:

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

31226 - HA availability status degraded

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

Recovery:

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

31227 - HA availability status failed

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

Recovery:

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

31228 - HA standby offline

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

Recovery:

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

31229 - HA score changed

Alarm Group:	HA
Description:	High availability health score changed
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

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

Recovery:

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

31231 - Platform alarm agent fault

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

Recovery:

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

31232 - Late heartbeat warning

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

Recovery:

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

31233 - HA Path Down

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

Recovery:

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

31234 - Untrusted Time Upon Initialization

Alarm Group:	REPL
Description:	Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction.

	Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolUtrustedTimeOnInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

31235 - Untrusted Time After Initialization

Alarm Group:	REPL
Description:	After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, etc. There are often accompanying Platform alarms to guide correction. Generally, applications remain running, but time-stamped data is likely incorrect, reports may be negatively affected, some behavior may be improper, etc.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	comcolUtrustedTimePostInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

31236 - HA Link Down

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

OID: comcolHaLinkDownNotify

Recovery:

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

31240 - Measurements collection fault

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

Recovery:

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

31250 - RE port mapping fault

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

Recovery:

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

31260 - SNMP Agent

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

Recovery:

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

31270 - Logging output

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

Recovery:

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

31280 - HA Active to Standby transition

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

OID:	comcolActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, it is recommended to contact *My Oracle Support (MOS)*.

31281 - HA Standby to Active transition

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

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, it is recommended to contact *My Oracle Support (MOS)*.

31282 - HA Management Fault

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

Recovery:

1. This alarm indicates an error occurred within the High Availability subsystem, but the system has automatically recovered.
2. If the alarm occurs frequently, it is recommended to contact *My Oracle Support (MOS)*.

31283 - Lost Communication with server

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

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

Recovery:

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

31285 - HA Node Join Recovery Entry

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

Recovery:

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

31286 - HA Node Join Recovery Plan

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

Recovery:

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

31287 - HA Node Join Recovery Complete

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

Recovery:

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

31290 - HA Process Status

Alarm Group:	HA
Description:	HA manager (cmha) status
Severity:	Info
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

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

Recovery:

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

31291 - HA Election Status

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

Recovery:

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

31292 - HA Policy Status

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

Recovery:

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

31293 - HA Resource Link Status

Alarm Group:	HA
Description:	HA ResourceAgent Link status
Severity:	Info

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

Recovery:

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

31294 - HA Resource Status

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

Recovery:

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

31295 - HA Action Status

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

Recovery:

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

31296 - HA Monitor Status

Alarm Group:	HA
Description:	HA Monitor action status

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

Recovery:

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

31297 - HA Resource Agent Info

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

Recovery:

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

31298 - HA Resource Agent Detail

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

Recovery:

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

31299 - HA Notification Status

Alarm Group:	HA

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

Recovery:

No action required.

31300 - HA Control Status

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

Recovery:

No action required.

31301 - HA Topology Events

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

Recovery:

No action required.

32113 - Uncorrectable ECC memory error

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

Recovery:

Contact the hardware vendor to request hardware replacement.

32114 - SNMP get failure

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

Recovery:

1. Verify device is active and responds to the ping command.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

32115 - TPD NTP Daemon Not Synchronized Failure

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

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedFailure
Alarm ID:	TKSPLATCR16

Recovery:

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

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

   a) Reset date:

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

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

32116 - TPD Server's Time Has Gone Backwards

Alarm Group:	PLAT
Description:	This alarm indicates that the server's current time precedes the timestamp of the last known time the servers time was good.
Severity:	Critical
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPTimeGoneBackwards
Alarm ID:	TKSPLATCR17

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.

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

2. If ntp peer is reachable, restart the ntpd service.
3. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

32117 - TPD NTP Offset Check Failure

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

Recovery:

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

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

   a) To reset date:

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

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

32300 - Server fan failure

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

Recovery:

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

32301 - Server internal disk error

Alarm Group:	PLAT
Description:	This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdIntDiskError
Alarm ID:	TKSPLATMA2

Recovery:

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

```
cat /proc/mdstat
```

```
cat /etc/raidtab
```

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

32303 - Server Platform error

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

Recovery:

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

```
cat /proc/mdstat
```

```
cat /etc/raidtab
```

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

32304 - Server file system error

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

Recovery:

1. Run syscheck in verbose mode.

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

32305 - Server Platform process error

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

Recovery:

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

32307 - Server swap space shortage failure

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

Recovery:

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

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

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

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

32308 - Server provisioning network error

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

Recovery:

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

32312 - Server disk space shortage error

Alarm Group:	PLAT
Description:	This alarm indicates that one of the following conditions has occurred: • A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system. • More than 90% of the total number of available files have been allocated on the file system.

- A file system has a different number of blocks than it had when installed.

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

Recovery:

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

32313 - Server default route network error

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

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

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

Recovery:

1. Run syscheck in verbose mode.

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

32314 - Server temperature error

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

Recovery:

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

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

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

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may

take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

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

32315 - Server mainboard voltage error

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

Recovery:

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

32316 - Server power feed error

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

Recovery:

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

32317 - Server disk health test error

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

Recovery:

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

32318 - Server disk unavailable error

Alarm Group:	PLAT

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

Recovery:

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

32320 - Device interface error

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

Recovery:

1. Run syscheck in verbose mode.
2. Investigate the failed bond, and slave devices, configuration:
    1. Navigate to /etc/sysconfig/network-scripts for the persistent configuration of a device.
3. Determine if the failed bond, and slave devices, has been administratively shut down or has operational issues:
    1. cat /proc/net/bonding/bondX, where X is bond designation
    2. ethtool <slave device>
4. If bond, and slaves, are healthy attempt to administratively bring bond up:
    1. ifup bondX

5. If the problem has not been resolved, it is recommended to contact *My Oracle Support (MOS)* and provide the system health check output and the output of the above investigation.

32321 - Correctable ECC memory error

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

Recovery:

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

32322 - Power Supply A error

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

Recovery:

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

32323 - Power Supply B error

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

Recovery:

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

32324 - Breaker panel feed error

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

Recovery:

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

3. If the problem has not been resolved, it is recommended to contact *My Oracle Support (MOS)* to request that the breaker panel be replaced.

32325 - Breaker panel breaker error

Alarm Group: PLAT

Description: This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see *Figure 2: Breaker Panel LEDs*) identify whether the fault occurred on the input power or the output power, as follows:

- A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit.

  Note: LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.

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

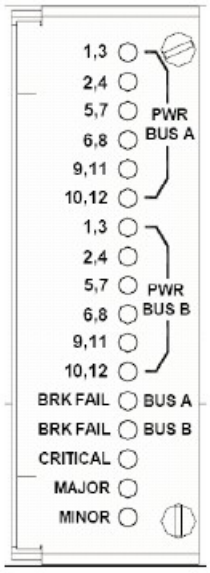

Figure 2: Breaker Panel LEDs

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 both servers. The single breaker panel normally sends alarm information to both servers:
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by both servers, go to the next step.
2. For each breaker assignment, verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

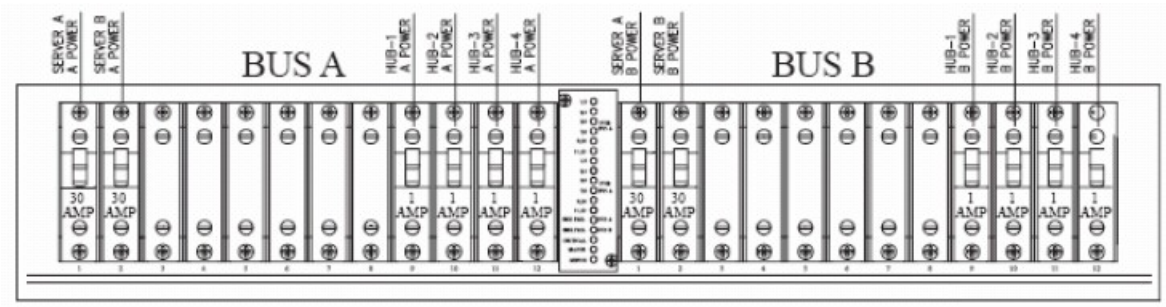

Figure 3: Breaker Panel Setting

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. Perform the following steps to correct this problem:

- Verify that the customer provided source for the affected power feed is operational. If the power source is properly functioning, have an electrician remove the plastic cover from the rear of the breaker panel and verify the power source is indeed connected to the input power feed connector on the rear of the breaker panel. Correct any issues found.
- Check the LEDs in the PWR BUS A group and the PWR BUS B group again.
  1. If the LEDs are now illuminated Green, the issue has been resolved. Proceed to step 4 to verify that the alarm has been cleared.
  2. If the LEDs are still illuminated Red, continue to the next sub-step.
- Have the electrician verify the integrity of the input power feed. The input voltage should measure nominally -48VDC (that is, between -41VDC and -60VDC). If the supplied voltage is not within the acceptable range, the input power source must be repaired or replaced.

  Note:

  Be sure the voltmeter is connected properly. The locations of the BAT and RTN connections are in mirror image on either side of the breaker panel.

  If the measured voltage is within the acceptable range, the breaker panel may be malfunctioning. The breaker panel must be replaced.

- Check the LEDs in the PWR BUS A group and the PWR BUS B group again after the necessary actions have been taken to correct any issues found

  1. If the LEDs are now illuminated Green, the issue has been resolved and proceed to step 4 to verify that the alarm has been cleared.
  2. If the LEDs are still illuminated Red, skip to step 5

3. Check the BRK FAIL LEDs for BUS A and for BUS B.

   - If one of the BRK FAIL LEDs is illuminated Red, then one or more of the respective Input Breakers has tripped. (A tripped breaker is indicated by the toggle located in the center position.) Perform the following steps to repair this issue:

   a) For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.
   b) After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, run syscheck and contact *My Oracle Support (MOS)*

4. If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise run syscheck and contact *My Oracle Support (MOS)*
5. Run syscheck.

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

32326 - Breaker panel monitoring error

Alarm Group:	PLAT
Description:	This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself. **Note:** When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm: • 32324 – Breaker panel feed error • 32325 – Breaker panel breaker error until the Breaker Panel Monitoring Error has been corrected.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	0 (zero)
OID:	tpdBrkPnlMntError
Alarm ID:	TKSPLATMA27

Recovery:

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

32327 - Server HA Keepalive error

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

Recovery:

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

   Note: This step may require command line ability.
4. It is recommended to contact *My Oracle Support (MOS)*.

32328 - DRBD is unavailable

Alarm Group:	PLAT

Description:	This alarm indicates that DRBD is not functioning properly on the local server. The DRBD state (disk state, node state, and/or connection state) indicates a problem.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdUnavailable
Alarm ID:	TKSPLATMA29

Recovery

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

32329 - DRBD is not replicating

Alarm Group:	PLAT
Description:	This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdNotReplicating
Alarm ID:	TKSPLATMA30

Recovery

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

32330 - DRBD peer problem

Alarm Group:	PLAT
Description:	This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdPeerProblem
Alarm ID:	TKSPLATMA31

Recovery

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

32331 - HP disk problem

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

Recovery:

1. Run syscheck in verbose mode.
2. If "Cache Status" is OK and "Cache Status Details" reports a cache error was detected so diagnostics should be run, there probably is no battery and data was left over in the write cache not getting flushed to disk and won't since there is no battery.
3. If "Cache Status" is "Permanently Disabled" and "Cache Status Details" indicated the cache is disabled, if there is no battery then the firmware should be upgraded.
4. Re-run syscheck in verbose mode if firmware upgrade was necessary.
5. If the condition persists, it is recommended to contact *My Oracle Support (MOS)* and provide the system health check output. The disk may need to be replaced.

32332 - HP Smart Array controller problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.
Severity:	Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHpDiskCtrlrProblem
Alarm ID:	TKSPLATMA33

Recovery:

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

32333 - HP hpacucliStatus utility problem

Alarm Group:	PLAT
Description:	This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus/hpDiskStatus daemon is either not running, or hung.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHPACUCLIProblem
Alarm ID:	TKSPLATMA34

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the HP disk status daemon is running. If not running verify that it was not administratively stopped.

   Note: The disk status daemon is named either TKLChpacucli or TPDhpDiskStatus in more recent versions of TPD.

   a) Executing "status TPDhpDiskStatus", or "status TKLChpacucli" depending on TPD release, should produce output indicating that the process is running.
4. If not running, attempt to start the HP disk status process :
   "start TPDhpDiskStatus", or if appropriate "start TKLChpacucli" .
5. Verify that there are no hpssacli, or hpacucli, error messages in /var/log/messages. If there are this could indicate that the HP utility is hung. If the HP hpssacli utility, or hpacucli utility, is hung, proceed with next step.

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

32334 - Multipath device access link problem

Alarm Group:	PLAT
Description:	One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdMpathDeviceProblem

Recovery:

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

32335 - Switch link down error

Alarm Group:	PLAT
Description:	The link is down.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSwitchLinkDownError
Alarm ID:	TKSPLATMA36

Recovery:

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, it is recommended to contact *My Oracle Support (MOS)* to determine who should verify port settings on both the server and the switch.

32336 - Half Open Socket Limit

Alarm Group:	PLAT

Description:	This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHalfOpenSockLimit
Alarm ID:	TKSPLATMA37

Recovery:

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

32337 - Flash Program Failure

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

Recovery:

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

32338 - Serial Mezzanine Unseated

Alarm Group:	PLAT
Description:	This alarm indicates that a connection to the serial mezzanine board may not be properly seated.
Severity:	Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSerialMezzUnseated
Alarm ID:	TKSPLATMA39

Recovery:

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

32339 - TPD Max Number Of Running Processes Error

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

Recovery:

1. Run syscheck in verbose mode.
2. Execute 'pstree' to see what pids are on the system and what process created them. Collect the output of command, and review the output to determine the process responsible for the alarm.
3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output, and pid output.

32340 - TPD NTP Daemon Not Synchronized Error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNotSynchronizedError
Alarm ID:	TKSPLATMA41

Recovery:

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

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

   a) To reset date:

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

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

32341 - TPD NTP Daemon Not Synchronized Error

Alarm Group:	PLAT
Description:	This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdNTPDaemonNeverSynchronized
Alarm ID:	TKSPLATMA42

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a) Ensure ntpd service is running.

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

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

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

   a) To reset date:

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

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

32342 - NTP Offset Check Error

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

Recovery:

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

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

a) To reset date:

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

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

32343 - TPD RAID disk

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

Recovery:

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

32344 - TPD RAID controller problem

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

Recovery:

1. Run syscheck in verbose mode.
2. Verify firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. It is recommended to contact *My Oracle Support (MOS)* and provide the system health check output.

32345 - Server Upgrade snapshot(s) invalid

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

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. If the alarm persists, it is recommended to contact *My Oracle Support (MOS)*.

32346 - OEM hardware management service reports an error

Alarm Group:	PLAT
Description:	This alarms indicates that OEM hardware management service reports an error.
Severity:	Major
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdOEMHardware
Alarm ID:	TKSPLATMA47

Recovery:

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

32347 - The hwmgmtcliStatus daemon needs intervention

Alarm Group:	PLAT
Description:	This alarms indicates the hwmgmtcliStatus daemon is not running or is not responding.
Severity:	Major

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHWMGMTCLIProblem
Alarm ID:	TKSPLATMA47

Recovery:

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

32348 - FIPS subsystem problem

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

32349 - File Tampering

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

Recovery:

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

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:

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

32500 - Server disk space shortage warning

Alarm Group:	PLAT
Description:	This alarm indicates that one of the following conditions has occurred: • A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system. • More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.
Severity:	Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskSpaceShortageWarning
Alarm ID:	TKSPLATMI1

Recovery:

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

32501 - Server application process error

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

Recovery:

1. Run syscheck in verbose mode.
2. If the alarm has been cleared, then the problem is solved.
3. If the alarm has not been cleared, determine the run level of the system.
   - If system run level is not 4, determine why the system is operating at that run level.
   - If system run level is 4, determine why the required number of instances processes are not running.
4. For additional assistance, it is recommended to contact *My Oracle Support (MOS)* and provide the syscheck output.

32502 - Server hardware configuration error

Alarm Group:	PLAT
Description:	This alarm indicates that one or more of the server's hardware components are not in compliance with specifications (refer to the appropriate hardware manual).
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHardwareConfigError
Alarm ID:	TKSPLATMI3

Recovery:

1. Run syscheck in verbose mode.
2. Contact the hardware vendor to request a hardware replacement.

32503 - Server RAM shortage warning

Alarm Group:	PLAT
Description:	This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdRamShortageWarning
Alarm ID:	TKSPLATMI4

Recovery

1. Refer to MPS-specific documentation for information regarding this alarm.
2. It is recommended to contact the *My Oracle Support (MOS)*.

32504 - Software Configuration Error

Alarm Group:	PLAT
Description:	This alarm is generated by the MPS syscheck software package and is not part of the PLAT distribution.

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

Recovery

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

32505 - Server swap space shortage warning

Alarm Group:	PLAT
Description:	This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time. **Note:** For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdSwapSpaceShortageWarning
Alarm ID:	TKSPLATMI6

Recovery:

1. Run syscheck in verbose mode.
2. Determine which processes are using swap.
   a) List application processes and determine the process id.
   b) Determine how much swap each process is using. One method to determine the amount of swap being used by process is:
   - grep VmSwap /proc/<process id>/status
3. It is recommended to contact *My Oracle Support (MOS)*, provide the system health check output, and process swap usage.

32506 - Server default router not defined

Alarm Group:	PLAT

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

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDefaultRouteNotDefined

Alarm ID: TKSPLATMI7

Recovery:

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

32507 - Server temperature warning

Alarm Group: PLAT

Description: This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID:	tpdServerTemperatureWarning
Alarm ID:	TKSPLATMI8

Recovery:

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

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

3. Run syscheck.
4. Replace the filter (refer to the appropriate hardware manual).

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

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

32508 - Server core file detected

Alarm Group:	PLAT
Description:	This alarm indicates that an application process has failed and debug information is available.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerCoreFileDetected
Alarm ID:	TKSPLATMI9

Recovery:

1. It is recommended to contact *My Oracle Support (MOS)* to create a service request.
2. On the affected server, execute this command:

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

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

3. Attach core files to the *My Oracle Support (MOS)* service request.

4. The user can remove the files to clear the alarm with this command:

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

32509 - Server NTP Daemon not synchronized

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

Recovery:

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

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

   a) To reset date:

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

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

32510 - CMOS battery voltage low

Alarm Group:	PLAT

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

Recovery:

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

32511 - Server disk self test warning

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

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact *My Oracle Support (MOS)*.

32512 - Device warning

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

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

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact *My Oracle Support (MOS)*.

32513 - Device interface warning

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

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact *My Oracle Support (MOS)*.

32514 - Server reboot watchdog initiated

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

Recovery:

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

32515 - Server HA failover inhibited

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

Recovery:

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

32516 - Server HA Active to Standby transition

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

Recovery:

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

32517 - Server HA Standby to Active transition

Alarm Group:	PLAT
Description:	This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.
Severity:	Minor

Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdHaStandbyToActiveTrans
Alarm ID:	TKSPLATMI18

Recovery:

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

32518 - Platform Health Check failure

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

Recovery:

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

32519 - NTP Offset Check failure

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

Recovery:

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

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

   a) To reset date:

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

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

32520 - NTP Stratum Check failure

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

Recovery:

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

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

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

   a) To reset date:

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

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

32521 - SAS Presence Sensor Missing

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

Recovery:

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

32522 - SAS Drive Missing

Alarm Group:	PLAT
Description:	This alarm indicates that the number of drives configured for this server is not being detected.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	sasDriveMissing
Alarm ID:	TKSPLATMI23

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

32523 - DRBD failover busy

Alarm Group:	PLAT
Description:	This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDrbdFailoverBusy
Alarm ID:	TKSPLATMI24

Recovery

A DRBD sync should not take more than 15 minutes to complete. Please wait for approximately 20 minutes, and then check if the DRBD sync has completed. If the alarm persists longer than this time period, it is recommended to contact *My Oracle Support (MOS)*.

32524 - HP disk resync

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

Recovery:

1. Run syscheck in verbose mode.
2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck.

3. If the alarm persists, it is recommended to contact *My Oracle Support (MOS)* and provide the syscheck output.

32525 - Telco Fan Warning

Alarm Group:	PLAT
Description:	This alarm indicates that the Telco switch has detected an issue with an internal fan.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdTelcoFanWarning
Alarm ID:	TKSPLATMI26

Recovery:

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

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

32526 - Telco Temperature Warning

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

Recovery:

1. Lower the ambient air temperature around the switch as low as possible.
2. If the problem persists, it is recommended to contact *My Oracle Support (MOS)*.

32527 - Telco Power Supply Warning

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

Recovery:

1. Verify the breaker was not tripped.
2. If the breaker is still good and problem persists, it is recommended to contact *My Oracle Support (MOS)* who can perform a `snmpget` command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 - Invalid BIOS value

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

Recovery:

Change the BIOS values to the expected values which involves re-booting the server. It is recommended to contact *My Oracle Support (MOS)* for directions on changing the BIOS.

32529 - Server Kernel Dump File Detected

Alarm Group:	PLAT

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

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact *My Oracle Support (MOS)*.

32530 - TPD Upgrade Failed

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

Recovery:

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

32531 - Half Open Socket Warning Limit

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

OID:	tpdHalfOpenSocketWarning
Alarm ID:	TKSPLATMI32

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact *My Oracle Support (MOS)*.

32532 - Server Upgrade Pending Accept/Reject

Alarm Group:	PLAT
Description:	This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdServerUpgradePendingAccept
Alarm ID:	TKSPLATMI33

Recovery:

Follow the steps in the application procedure to accept or reject the upgrade.

32533 - TPD Max Number Of Running Processes Warning

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

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact *My Oracle Support (MOS)*.

32534 - TPD NTP Source Is Bad Warning

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

Recovery:

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

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

   a) To reset date:

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

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

32535 - TPD RAID disk resync

Alarm Group:	PLAT
Description:	This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdDiskResync
Alarm ID:	TKSPLATMI36

Recovery:

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

32536 - TPD Server Upgrade snapshot(s) warning

Alarm Group:	PLAT
Description:	This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal
Auto Clear Seconds:	0 (zero)
OID:	tpdUpgradeSnapshotWarning
Alarm ID:	TKSPLATMI37

Recovery:

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

32537 - FIPS subsystem warning event

Alarm Type:	PLAT
Description:	This alarm indicates that the FIPS subsystem requires a reboot in order to complete configuration.
Severity:	Minor
Instance:	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score:	Normal

Auto Clear Seconds:	0 (zero)
OID:	tpdFipsSubsystemWarning

Recovery

If alarm doesn't clear on its own, it is recommended to contact *My Oracle Support (MOS)*.

32540 - CPU Power limit mismatch

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

Recovery:

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

32700 - Telco Switch Notification

Alarm Group:	PLAT
Description	Telco Switch Notification
Severity	Info
Instance	May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score	Normal
Auto Clear Seconds	86400
OID	tpdTelcoSwitchNotification

Recovery:

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

32701 - HIDS Initialized

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

OID: tpdHidsBaselineCreated

Recovery:

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

32702 - HIDS Baseline Deleted

Alarm Group: PLAT

Description: HIDS baseline was deleted.

Default Severity: Info

OID: tpdHidsBaselineDeleted

Recovery:

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

32703 - HIDS Enabled

Alarm Group: PLAT

Description: HIDS was enabled.

Default Severity: Info

OID: tpdHidsEnabled

Recovery:

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

32704 - HIDS Disabled

Alarm Group: PLAT

Description: HIDS was disabled.

Default Severity: Info

OID: tpdHidsDisabled

Recovery:

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

32705 - HIDS Monitoring Suspended

Alarm Group: PLAT

Description: HIDS monitoring suspended.

Default Severity: Info

OID: tpdHidsSuspended

Recovery:

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

32706 - HIDS Monitoring Resumed

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

Recovery:

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

32707 - HIDS Baseline Updated

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

Recovery:

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

QP (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:

1. This alarm automatically clears as Policy processes are restarted.
2. 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/Al

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	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. Running cluster configuration: • 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	A scheduled backup failed to synchronize the local server-backup archive with the remote server-backup archive. • Hostname=<hostname | IPaddr> • path=<path> • errorcode=<rsync error>
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 64800 seconds (18 hours).
OID	QPServerBackupRsyncFailed

Recovery:

Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

70011 – QP Failed System-backup Remote Archive Rsync

Alarm Type	QP
Description	A scheduled backup failed to synchronize the local system-backup archive with the remote system-backup archive. Hostname=<host name | IP addr>, user=<user>, 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	QPSystemBackupRsyncFailed

Recovery:

Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

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:

Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

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:

Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

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:

- 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 route configuration and check the STATIC IP status.
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 secondary server is in the same cluster (the most common case), perform a failover by restarting the current active blade. If the best secondary server 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)*.

70027 – QP Server Network Config Error

Alarm Type	QP
Description	QP Server Network Error.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	Autoclears in 1800 seconds (30 minutes).
OID	QPServerNetworkConfigError

Recovery

1. Correct the indicated networking configuration.
2. If the problem persists, 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 `qp_hamonitor` has detected the VIP is not defined on this bonded network interface; VIP is defined on this bonded network interface and `qp_hamonitor` process has detected the interface is up.
OID	QPBondedInterfaceDown

Recovery:

1. Reset the OAM network interface and run process `qp_hamonitor` to clear the alarm.
2. If the `qp_hamonitor` process does not clear the alarm, or if the alarm does not clear automatically, or if the alarm is persists, contact *My Oracle Support (MOS)*

70029 – QP peer node bonded interface is down

Alarm Type	QP
Description	QP Peer Node ${*host name*} (${*ip addr*}) bonded interface bond0 (OAM) is down.
Default Severity	Critical
Instance	Peer_OAM
HA Score	Normal
Clearing Action	Process `qp_hamonitor` will clear the alarm once the OAM network interface is up. The alarm will also clear automatically after 60 seconds.
OID	QPPeerBondedInterfaceDown

Recovery:

1. Reset the OAM network interface and run process `qp_hamonitor` to clear the alarm.
2. If the `qp_hamonitor` process does not clear the alarm, or if the alarm does not clear automatically, or if the alarm is persists, contact *My Oracle Support (MOS)*

70030 – QP backplane bonded interface is down

Alarm Type	QP
Description	Backplane bonded interface is down.
Default Severity	Critical
Instance	Backplane_bond3
HA Score	Normal
Clearing Action	Process `qp_hamonitor` has detected the bonded backplane network interface has been restored or the alarm has been raised for 60 seconds.
OID	QPBackplaneBondedInterfaceDown

Recovery:

Restore the bonded backplane network interface that is down and the `qp_hamonitor` process will clear the alarm.

70031 – QP degrade because one or more interfaces are down

Alarm Type	QP

Description	HA status is degraded because selected interface(s) (${*OAM, SIGA, or SIGB*}) are down.
Default Severity	Critical
Instance	OAM or SIGA or SIGB
HA Score	Failed
Clearing Action	Alarm clears when process `qp_hamonitor` has detected all OAM, SIGA and SIGB network interfaces are up. Alarm also clears automatically after 60 seconds.
OID	QPInterfacesDegrade

Recovery:

1. Reset the interfaces that are down and run the `qp_hamonitor` process to clear the alarm.
2. If this does not clear the alarm, or if the alarm does not automatically clear, or if the alarm persists, 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 `qpIPv4Harvest --block_oam_ipv4` is finished successfully, this alarm is raised.
Default Severity	Minor
Instance	N/A
HA Score	Normal

Clearing Action	This alarm is cleared by `qpIPv4Harvest –harvest_oam_only` or `qpIPv4Harvest –harvest_oam_all`.
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 `qpIPv4Harvest –block_all_ipv4` is finished successfully, this alarm is raised.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm is cleared by `qpIPv4Harvest –harvest_all`.
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 `qpIPv4Harvest –block_oam_ipv4` 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 `qpIPv4Harvest –block_all_ipv4` 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.

70045 – DNS Server is not available

Alarm Type	QP
Description	If DNS servers are configured on PCRF nodes, those nodes will use DNS servers. Process qp_monitor will check DNS availability at the runtime of every node. If a DNS server is found unavailable, QP alarm 70045 is triggered.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	This alarm will be cleared automatically after 120 seconds.
OID	QPDNSServerIsNotAvailable

Recovery:

1. If the alarm message is **No reply from server**, the server could not be reached or the connection has timed out. To resolve:
   a) Check the route and firewall settings from the PCRF node reporting the alarm to determine if a DNS server can be accessed.
   b) Repair the access to the specific DNS server.
2. If the alarm message is **Internal error** the DNS server IP address format is incorrect. To resolve:

a) Use Platcfg commands `Policy Configuration -> Perform Initial Configuration` to check the IP address format of the DNS server:

70050 – QP Timezone change detected

Alarm Type	QP
Description	Time zone has been changed using `platcfg` commands `Server Configuration -> Time Zone -> Edit`. The application needs to be restarted after this change.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears when the application is restarted (`qp_procmgr` restarted). This is not an auto-clear alarm.
OID	QPTimezonechangedetected

Recovery:

1. Log in to the server with root privileges.
2. Execute the command `service qp_procmgr restart`.
3. If the alarm persists, collect savelogs and 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. Click **Alarm Details** associated with the alarm in the CMP GUI to find the root cause of the failed upgrade action.
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	UpgradeOperationFailed

Recovery:

1. Make changes as detailed in the **Alarm Detail** associated with the alarm and then re-attempt the failed upgrade action.
2. If the issues cannot be resolved, collect savelogs and 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:

1. If alarm 70506 is also triggered, make changes as detailed in the **Alarm Detail** associated with alarm 70506 and then re-attempt the failed upgrade action to resolve both alarms.
2. If the alarm persists, collect savelogs and 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 or when OM statistics are run again.
OID	OmStatsParseError

Recovery:

Check to ensure Policy server version is the same as the CMP version. If the versions are different, upgrade the server version to be the same as the CMP version.

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) or when OM statistics are run again.
OID	OmStatsExceptionError

Recovery:

1. Check to ensure Policy server version is the same as the CMP version. If the versions are different, upgrade the server version to be the same as the CMP version.
2. Check MySQL status to ensure there is not an exception in the DC log.

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 or when OM statistics are run again.
OID	OmStatsValueExceedError

Recovery:

Check whether the list of IP addresses in a Network Element Diameter SCTP connection association value exceeds 255 in length. If found, correct the value length.

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:

1. Check configuration and availability of the downstream element.
2. Check the downstream element for a reboot or other service interruption.
3. .If the downstream element has not failed, make sure that the network path from the MPE device to the downstream element is operational.
4. 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	Alarm clears when the connection to a remote peer is restored. The alarm also clears automatically after 7200 seconds.
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:

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

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 `RC.TrapNoPcefEnabled` to true in `RcMgr`. This update occurs in both the MPE-R and MPE-S. The SubId 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 GateSet/GateInfo/GateDelete.
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 *ip-addr* has reached the configured maximum number of upstream gates.

Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 60 seconds.
OID	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 *ip-addr* has reached the configured maximum grants per interval on all upstream gates.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	This alarm clears automatically after 60 seconds.
OID	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 *{IP Address}*.
Default Severity	Minor
Instance	*{host name of MTA}*
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 – Policy Notification:Lost connection with destination URL

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 (*{external system IP}*, *{external system IP}*, 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:

1. Check all enabled Stats Files Synchronization tasks status in the DC (Data Collection) tasks of CMP system and ensure they are configured successfully.
2. Exchange SSL key with mate server in cluster.

74021 – Files Synchronization Failure

Alarm Type	PCRF
Description	Files synchronization failure. Files Synchronization #*{num}* task failed to synchronize local to remote server (*{external system Host Name/IP}*) after retry *{num}* times, where: • *{num}* is task # • *{num}*is retry times (1 to 5) • *{external system Host Name/IP}* 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 *FTP server Host Name/IP* after retry *number* 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 *configured threshold value* at *site name.*
Default Severity	Major
Instance	N/A
HA Score	Normal

Clearing Action	This alarm clears when the number of failed MPE pairs remain at a lower value than the threshold of *max primary site failure threshold* at *site*, or clears automatically after 30 minutes (1800 seconds).
OID	QPMaxMPEPrimaryClusterFailure

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	Major
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	Major
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 be cleared when the issue is fixed internally on the affected blades.
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)*.

78850 - VNF operation error

Alarm Type	PCRF
Description	There was an error while performing the requested operation on the VNF cluster.
Default Severity	Minor
Instance	N/A
HA Score	Normal
Clearing Action	The event will clear when the VM is in the Active state or the event must be cleared manually.
OID	VNFOperationError

Recovery:

Trace Logs provide details of the operation failure and which VMs were impacted. Validate information that was submitted as part of the request. Correct Topology and repeat the failed operation or take corrective action on the VM directly.

79002 - Sess 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 Exceed

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 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 Exceed

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	AvgBindSizeReachedThreshold

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	This alarm clears automatically after 30 seconds or when the Mediation load recovers.
OID	MediationSOAPTooBusy

Recovery:

1. Check that OCUDR is in a normal state to handle a SOAP provisioning request.
2. 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	This alarm clears when provisioning the connection between the Mediation and OCUDR recovers.
OID	SPRConnectionFailed

Recovery:

1. Check that the provisioning data source configuration on the Mediation server is correct.
2. 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	This alarm clears automatically after 3600 seconds or when the disk usage of the Mediation server is decreased to value less than the quota limit.
OID	MSDiskQuotaExceed

Recovery:

1. Release disk usage to ensure that 32G of free disk space is available in the sync directory.
2. 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	This alarm clears when the disk space is not fully used.
OID	MSDiskNoSpace

Recovery:

1. Release disk usage to ensure that 32G of free disk space is available in the sync directory.
2. 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 - Files Uploading Failure

Alarm Type	PCRF
Description	SMS Notification Statistics Upload Task failed to upload stats files to remote FTP server after retry.
Default Severity	Major
Instance	N/A
HA Score	Normal
Clearing Action	Auto clears after 300 seconds or the next time the task is run.
OID	FilesUploadingFailure

Recovery:

1. Check the FTP server configuration is correct in schedule task *SMS Notification Statistics Uploading Task*.
2. Check and ensure remote FTP server is accessible and service is available.

79120 - Batch Disk Quota Exceeds

Alarm Type	PCRF
Description	The batch folder disk quota exceeds.
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:

1. Check if the X1 Connection is down.
2. 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:

1. Check if the X2 Connection is down.
2. 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 `qp-procmgr` as `qp-procmgr` shuts down.
OID	QPDBStateChange

Recovery:

Because this is an information-only message, there is no recovery 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. Recovery is immediate.

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. Recovery is immediate.

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. Recovery is immediate.

86200 - CMP User Promoted Server

Alarm Type	PCRF
Description	CMP user promoted server. The current site becomes the Primary site.
Default Severity	Info

Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserPromotedServer

Recovery:

No action required. Recovery is immediate.

86201 - CMP User Demoted Server

Alarm Type	PCRF
Description	CMP user demoted server. The current site becomes the Secondary site.
Default Severity	Info
Instance	N/A
HA Score	Normal
Clearing Action	N/A
OID	CMPUserDemotedServer

Recovery:

No action required. Recovery is immediate.

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 raise 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:

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::diameterOMAAARecvSuccess.0 = Counter32: 0
TKLC-APP-MIB::diameterOMAAARecvFailure.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::diameterOMSTARecvSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMSTARecvFailure.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::diameterOMASARecvSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMASARecvFailure.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::diameterOMRAARecvSuccess.0 = Counter32:
TKLC-APP-MIB::diameterOMRAARecvFailure.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

Glossary

A

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

B

B-RAS	Broadband Remote Access Server 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.

C

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

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	Network Configuration Management Platform The NW-CMP server configures Network tier objects. Examples of Network tier objects are policies, network elements, and configuration templates.

O

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