# Oracle®Communications Policy Management

SNMP User's Guide

Release 12.0

**E60244 Revision 01**

March 2015

ORACLE®

Oracle®Communications SNMP User's Guide, Release 12.0

# 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 using CMP.
- *Supported MIBs* describes the MIBs that are supported for SNMP.
- *Support for Traps* describes the Policy Management functioning of alarms and traps with SNMP.

## Scope and Audience

This guide is intended for system integrators and other qualified service personnel responsible for managing a Policy Management system.

## Documentation Admonishments

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

**Table 1: Admonishments**

| Icon | Description |
|---|---|
|  | **Danger**:<br>(This icon and text indicate the possibility of *personal injury*.) |
|  | **Warning**:<br>(This icon and text indicate the possibility of *equipment damage*.) |
|  | **Caution**:<br>(This icon and text indicate the possibility of *service interruption*.) |

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

## Related Publications

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

## Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 *www.adobe.com*.

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Select the **Applications** tile.
   The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

## 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 "walk" through 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.

### SNMP Extension

SNMP provides the ability to augment the standard set of MIB objects with new values specific for certain applications and devices. New functions can continuously be added to SNMP, using a standard method defined to incorporate that function into SNMP devices and network managers. Adding new functions is accomplished through the process of "compiling" a new MIB, which allows the user to add new MIB definitions to the system. The definitions are usually supplied by network equipment vendors in specially formatted text files using the ASN.1 standard syntax. (ASN.1 refers to "Abstract Syntax Notation One", which is a type declaration language adopted by SNMP and used a few other places, including encryption and CMIP protocols.)

The MIB of an SNMP device is usually fixed; it is constructed by the network equipment vendor (such as a router manufacturer or computer hardware vendor) and cannot be added to or modified. The extension of SNMP refers strictly to SNMP management software, which can become aware of the MIB values supported by the device by compiling a description of the device into the network management program.

# Chapter 3

# Configuring SNMP

**Topics:**



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

# 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 Application Network and stored on the CMP servers. 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/MRAto the CMP, SNMP can be configured in either of 2 ways:

- The Policy system can be configured so that the CMP is the source of all traps.
- The Policy systems can be configured to allow each server to generate its own traps and deliver them to the SNMP management servers.

*Figure 1: SNMP Configuration* illustrates the two SNMP configurations.

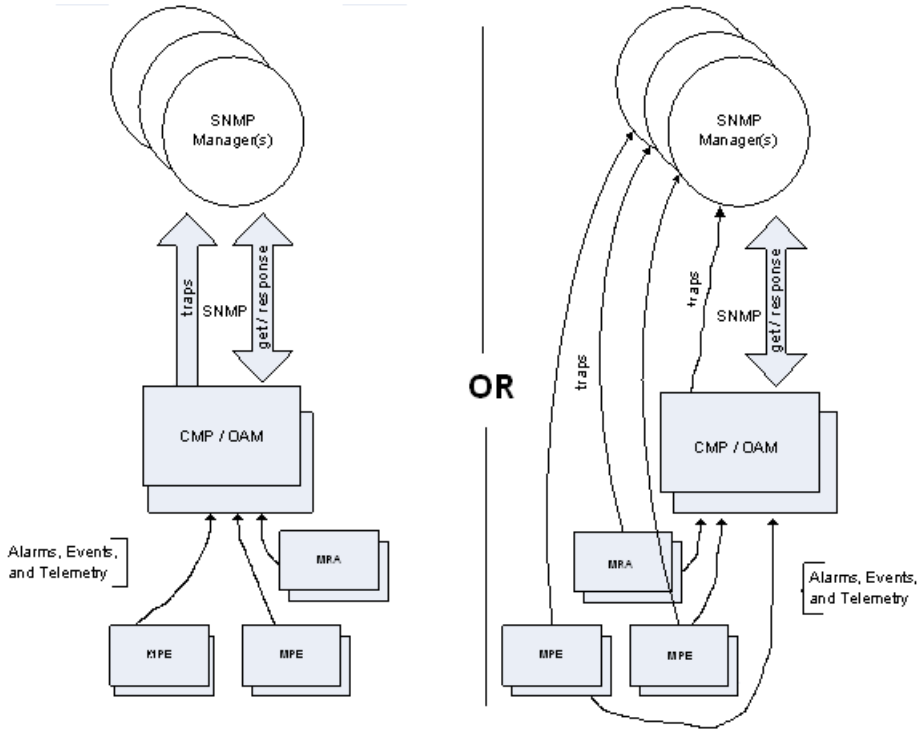


**Figure 1: SNMP Configuration**

On the SNMP Settings Edit page, the check box labeled "Traps from individual Servers" determines the mode in which the SNMP notifications will operate. When the box is checked to have each server generate traps, the Policy systems will operate as shown in the right-hand side of *SNMP Configuration*.

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

### SNMP Versions

SNMP version 2c (SNMPv2c) and SNMP version 3 (SNMPv3) are supported. SNMP version 1 (SNMPv1) is not supported. On the SNMP Setting Edit page:

- When you configure SNMPv2c, you must use a community that is not "public" or "private".
- When you configure SNMPv3, you must enter an "Engine ID", and a "username" and "password" for the SNMPv3 user.

## Configuring SNMP Settings

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

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

To configure SNMP settings:

1. Log in to the CMP system from its server address as a user with administrator privileges.

   The navigation pane is displayed.

2. From the **Platform Setting** section of the navigation pane, select **SNMP Setting**.

   The **SNMP Settings** page displays.

3. Click **Modify**.

   The **SNMP Settings** page opens.

4. Edit the settings.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

*Table 2: SNMP Attributes* describes the SNMP attributes that can be edited.

**Table 2: SNMP Attributes**

| Field Name | Description |
|---|---|
| Manager 1-5 | SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IPv4/IPv6 address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. Port configuration is optional for each manager and it can have a value between 1 and 65535. If it is not configured and left blank, the port defaults to 162.<br><br>By default, these fields are blank.<br><br>**Note:** The IPv6 address is not supported. |
| Enabled Versions | Supported SNMP versions:<br>• **SNMPv2c**<br>• **SNMPv3** |

| Field Name | Description |
|---|---|
| | • **SNMPv2c and SNMPv3 (default)** |
| Traps Enabled | Enable the sending SNMPv2 traps (default is enabled).<br>**Note:** This option must be selected to use the SNMP Trap Forwarding feature.<br>Clear the checkbox to disable sending SNMPv2 traps. |
| Traps from individual Servers | Enable sending traps from an individual server (default is disabled).<br>**Note:** To use the SNMP Trap Forwarding feature, ensure that this option is not selected.<br>Clear the checkbox to send traps from the active CMP system only. |
| SNMPv2c Community Name | The SNMP read-write community string.<br>The field is required if SNMPv2c is enabled.<br>The name can contain alphanumeric characters and cannot exceed 31 characters in length.<br>The name cannot be either **`private`** or **`public`**.<br>The default value is **`snmppublic`**. |
| SNMPv3 Engine ID | Configured Engine ID for SNMPv3.<br>The field is required If SNMPv3 is enabled.<br>The Engine ID includes only hexadecimal digits (0-9 and a-f).<br>The length can be from 10 to 64 digits.<br>The default is no value (empty). |
| SNMPv3 Security Level | SNMPv3 Authentication and Privacy options are:<br>1. **No Auth No Priv** — Authenticate using the Username. No Privacy.<br>2. **Auth No Priv** — Authentication using MD5 or SHA1 protocol.<br>3. **Auth Priv** — Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol.<br>The default value is **Auth Priv**. |
| SNMPv3 Authentication Type | Authentication protocol for SNMPv3. Options are:<br>1. **SHA-1** — Use Secure Hash Algorithm authentication.<br>2. **MD5** — Use Message Digest authentication.<br>The default value is **SHA-1**. |
| SNMPv3 Privacy Type | Privacy Protocol for SNMPv3. Options are:<br>1. **AES** — Use Advanced Encryption Standard privacy.<br>2. **DES** — Use Data Encryption Standard privacy. |

| Field Name | Description |
|---|---|
| | The default value is **AES**. |
| SNMPv3 Username | The SNMPv3 User Name.<br>The field is required if SNMPv3 is enabled.<br>The name must contain alphanumeric characters and cannot not exceed 32 characters in length.<br>The default value is **`TekSNMPUser`**. |
| SNMPv3 Password | Authentication password for SNMPv3. This value is also used for msgPrivacyParameters.<br>The field is required If SNMPv3 is enabled.<br>The length of the password must be between 8 and 64 characters; it can include any character.<br>The default value is **`snmpv3password`**. |

## Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network.

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

The SNMP Trap Forwarding feature, which allows the CMP system to be used to forward SNMP traps, is enabled using these settings. See *Table 3: SNMP Attributes* for information on the settings used to enable this feature.

To configure SNMP settings:

1. Log in to the CMP system from its server address as the Administration user.

   The navigation pane is displayed.

2. From the **Platform Setting** section of the navigation pane, select **SNMP Setting**.

   The SNMP Settings attributes are displayed.

3. Click **Modify**.

   The **SNMP Settings** page opens.

4. Edit the settings that need to be entered or changed.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

*Table 3: SNMP Attributes* describes the SNMP attributes that can be edited.

**Table 3: SNMP Attributes**

| Field Name | Description |
|---|---|
| Manager 1-5 | SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IPv4 address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. The field is required to allow the Manager to receive traps.<br>By default, these fields are empty.<br>**Note:** The IPv6 address is not supported. |
| Enabled Versions | Supported SNMP versions:<br>• SNMPv2c<br>• SNMPv3<br>• SNMPv2c and SNMPv3 (default) |
| Traps Enabled | Enable sending SNMPv2 traps (default is box check marked)<br>**Important:** This option must be check marked to use the SNMP Trap Forwarding feature.<br>Disable sending SNMPv2 traps (box not check marked) |
| Traps from individual Servers | Enable sending traps from an individual server (box check marked).<br>Send traps only from the active CMP system (default is box not check marked)<br>**Important:** To use the SNMP Trap Forwarding feature, ensure that this option is NOT check marked. |
| SNMPv2c Community Name | The SNMP read-write community string.<br>The field is required if SNMPv2c is enabled.<br>The name can contain alphanumeric characters and cannot exceed 31 characters in length.<br>The name cannot be either “private” or “public”.<br>The default value is “snmppublic”. |

| Field Name | Description |
|---|---|
| SNMPv3 Engine ID | Configured Engine ID for SNMPv3.<br>The field is required If SNMPv3 is enabled.<br>The Engine ID includes only hexadecimal digits (0-9 and a-f).<br>The length can be from 10 to 64 digits.<br>The default is no value (empty). |
| SNMPv3 Security Level | SNMPv3 Authentication and Privacy options.<br>**1.** "No Auth No Priv" - Authenticate using the Username. No Privacy.<br>**2.** "Auth No Priv" - Authentication using MD5 or SHA1 protocol.<br>**3.** "Auth Priv" - Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol.<br>The default value is "Auth Priv". |
| SNMPv3 Authentication Type | Authentication protocol for SNMPv3. Options are:<br>**1.** "SHA-1" - Use Secure Hash Algorithm authentication.<br>**2.** "MD5" - Use Message Digest authentication.<br>The default value is "SHA-1". |
| SNMPv3 Privacy Type | Privacy Protocol for SNMPv3. Options are:<br>**1.** "AES": Use Advanced Encryption Standard privacy.<br>**2.** "DES": Use Data Encryption Standard privacy.<br>The default value is "AES". |
| SNMPv3 Username | The SNMPv3 User Name.<br>The field is required if SNMPv3 is enabled.<br>The name must contain alphanumeric characters and cannot not exceed 32 characters in length.<br>The default value is "TekSNMPUser." |
| SNMPv3 Password | Authentication password for SNMPv3. This value is also used for msgPrivacyParameters.<br>The field is required If SNMPv3 is enabled.<br>The length of the password must be between 8 and 64 characters; it can include any character.<br>The default value is "snmpv3password". |

# Configuring SNMP Settings

You can configure SNMP settings for the CMP system and all Policy Management servers in the topology network.

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

The SNMP Trap Forwarding feature, which allows the CMP system to be used to forward SNMP traps, is enabled using these settings. See *Table 4: SNMP Attributes* for information on the settings used to enable this feature.

To configure SNMP settings:

1. Log in to the CMP system from its server address as the Administration user.

   The navigation pane is displayed.

2. From the **Platform Setting** section of the navigation pane, select **SNMP Setting**.

   The SNMP Settings attributes are displayed.

3. Click **Modify**.

   The **SNMP Settings** page opens.

4. Edit the settings that need to be entered or changed.
5. When you finish, click **Save** (or **Cancel** to discard your changes).

*Table 4: SNMP Attributes* describes the SNMP attributes that can be edited.

**Table 4: SNMP Attributes**

| Field Name | Description |
|---|---|
| Manager 1-5 | SNMP Manager to receive traps and send SNMP requests. Each Manager field can be filled as either a valid host name or an IPv4 address. A hostname should include only alphanumeric characters. Maximum length is 20 characters, and it is not case-sensitive. This field can also be an IP address. An IP address should be in a standard dot-formatted IP address string. The field is required to allow the Manager to receive traps.<br>By default, these fields are empty.<br>**Note:** The IPv6 address is not supported. |
| Enabled Versions | Supported SNMP versions:<br>• SNMPv2c<br>• SNMPv3<br>• SNMPv2c and SNMPv3 (default) |

| Field Name | Description |
|---|---|
| Traps Enabled | Enable sending SNMPv2 traps (default is box check marked)<br><br>**Important:** This option must be check marked to use the SNMP Trap Forwarding feature.<br><br>Disable sending SNMPv2 traps (box not check marked) |
| Traps from individual Servers | Enable sending traps from an individual server (box check marked).<br><br>Send traps only from the active CMP system (default is box not check marked)<br><br>**Important:** To use the SNMP Trap Forwarding feature, ensure that this option is NOT check marked. |
| SNMPv2c Community Name | The SNMP read-write community string.<br><br>The field is required if SNMPv2c is enabled.<br><br>The name can contain alphanumeric characters and cannot exceed 31 characters in length.<br><br>The name cannot be either “private” or “public”.<br><br>The default value is “snmppublic”. |
| SNMPv3 Engine ID | Configured Engine ID for SNMPv3.<br><br>The field is required If SNMPv3 is enabled.<br><br>The Engine ID includes only hexadecimal digits (0-9 and a-f).<br><br>The length can be from 10 to 64 digits.<br><br>The default is no value (empty). |
| SNMPv3 Security Level | SNMPv3 Authentication and Privacy options.<br><br>1. “No Auth No Priv” - Authenticate using the Username. No Privacy.<br>2. “Auth No Priv” - Authentication using MD5 or SHA1 protocol.<br>3. “Auth Priv” - Authenticate using MD5 or SHA1 protocol. Encrypt using the AES and DES protocol.<br><br>The default value is “Auth Priv”. |

| Field Name | Description |
|---|---|
| SNMPv3 Authentication Type | Authentication protocol for SNMPv3. Options are:<br>**1.** "SHA-1" - Use Secure Hash Algorithm authentication.<br>**2.** "MD5" - Use Message Digest authentication.<br>The default value is "SHA-1". |
| SNMPv3 Privacy Type | Privacy Protocol for SNMPv3. Options are:<br>**1.** "AES": Use Advanced Encryption Standard privacy.<br>**2.** "DES": Use Data Encryption Standard privacy.<br>The default value is "AES". |
| SNMPv3 Username | The SNMPv3 User Name.<br>The field is required if SNMPv3 is enabled.<br>The name must contain alphanumeric characters and cannot not exceed 32 characters in length.<br>The default value is "TekSNMPUser." |
| SNMPv3 Password | Authentication password for SNMPv3. This value is also used for msgPrivacyParameters.<br>The field is required If SNMPv3 is enabled.<br>The length of the password must be between 8 and 64 characters; it can include any character.<br>The default value is "snmpv3password". |

# 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 portions of the SNMP MIB, and object subsets, to be referenced. 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 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

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/mib`

  `(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/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 Policy Management functioning of alarms and traps with SNMP.

## Alarms Overview

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

- Critical
- Major
- Minor

Policy Server alarms are generated by MPE or MRA servers 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 (Are explicitly "set" and "cleared")
  - Have a Severity: Critical, Major, Minor
  - Will cause a trap
- Events
  - Are issued with a Condition is detected (not a Fault)
  - Are not latched (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)*.

## Platform (31000-32700)

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

### 31000 - S/W Fault

**Alarm Type:** SW

**Description:** Program impaired by s/w fault

**Default Severity:** Minor

**OID:** comcolSwFaultNotify

**Recovery:**

1. Export event history for the given server and the given process.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31001 - S/W Status

**Alarm Type:** SW

**Description:** Program status

**Default Severity:** Info

**OID:** comcolSWStatusNotify

**Recovery:**

No action required.

### 31002 - Process Watchdog Failure

**Alarm Type:** SW

**Description:** Process watchdog timed out

**Default Severity:** Minor

**OID:** comcolProcWatchdogFailureNotify

**Recovery:**

1. Export event history for the given server and the given process.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31003 - Thread Watchdog Failure

**Alarm Type:** SW

**Description:** Thread watchdog timed out

**Default Severity:** Minor

**OID:** comcolThreadWatchdogFailureNotify

**Recovery:**

1. Export event history for the given server and the given process.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31100 - DB Replication Fault

**Alarm Type:** SW

**Description:** The DB replication process is impaired by a s/w fault.

**Default Severity:** Minor

**OID:** comcolDbReplicationFaultNotify

**Recovery:**

1. Export event history for the given server.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31101 - DB Replication To Slave Failure

**Alarm Type:** REPL

**Description:** DB replication to a slave DB has failed

**Default Severity:** Minor

**OID:** comcolDbRepToSlaveFailureNotify

**Recovery:**

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

### 31102 - DB Replication From Master Failure

**Alarm Type:** REPL

**Description:** DB replication from a master DB has failed

**Default Severity:** Minor

**OID:** comcolDbRepFromMasterFailureNotify

**Recovery:**

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

## 31103 - DB Replication Update Fault

**Alarm Type:** REPL

**Description:** DB replication process cannot apply update to DB

**Default Severity:** Minor

**OID:** comcolDbRepUpdateFaultNotify

**Recovery:**

1. Export event history for the given server and inetsync task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 31104 - DB Replication Latency Over Threshold

**Alarm Type:** REPL

**Description:** DB replication latency has exceeded thresholds

**Default Severity:** Minor

**OID:** comcolDbRepLatencyNotify

**Recovery:**

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

## 31105 - DB Merge Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolDbMergeFaultNotify

**Recovery:**

1. Export event history for the given server and inetmerge task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 31106 - DB Merge To Parent Failure

**Alarm Type:** COLL

**Description:** DB merging to the parent Merge Node has failed

**Default Severity:** Minor

**OID:** comcolDbMergeToParentFailureNotify

**Recovery:**

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

### 31107 - DB Merge From Child Failure

**Alarm Type:** COLL

**Description:** DB merging from a child Source Node has failed

**Default Severity:** Minor

**OID:** comcolDbMergeFromChildFailureNotify

**Recovery:**

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

### 31108 - DB Merge Latency Over Threshold

**Alarm Type:** COLL

**Description:** DB Merge latency has exceeded thresholds

**Default Severity:** Minor

**OID:** comcolDbMergeLatencyNotify

**Recovery:**

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

### 31109 - Topology Config Error

**Alarm Type:** DB

**Description:** Topology is configured incorrectly

**Default Severity:** Minor

**OID:** comcolTopErrorNotify

**Recovery:**

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

### 31110 - DB Audit Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolDbAuditFaultNotify

**Recovery:**

1. Export event history for the given server and idbsvc task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31111 - DB Merge Audit in Progress

**Alarm Type:** COLL

**Description:** DB Merge Audit between mate nodes in progress

**Default Severity:** Minor

**OID:** comcolDbMergeAuditNotify

**Recovery:**

No action required.

### 31112 - DB Replication Update Log Transfer Timed Out

**Alarm Type:** REPL

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

**Default Severity:** Minor

**OID:** comcolDbRepUpLogTransTimeoutNotify

**Recovery:**

No action required. If the problem persists, contact *My Oracle Support (MOS)* if this occurs frequently.

### 31113 - DB Replication Manually Disabled

**Alarm Type:** REPL

**Description:** Replication Manually Disabled

**Default Severity:** Minor

**OID:** comcolDbReplicationManuallyDisabledNotify

**Recovery:**

No action required.

### 31114 - DB Replication over SOAP has failed

**Alarm Type:** REPL

**Description:** DB replication of configuration data via SOAP has failed

**Default Severity:** Minor

**OID:** comcolDbReplicationSoapFaultNotify

**Recovery:**

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

### 31115 - DB Service Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolDbServiceFaultNotify

**Recovery:**

1. Export event history for the given server and idbsvc task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31116 - Excessive Shared Memory

**Alarm Type:** MEM

**Description:** The amount of shared memory consumed exceeds configured thresholds

**Default Severity:** Major

**OID:** comcolExcessiveSharedMemoryConsumptionNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31117 - Low Disk Free

**Alarm Type:** DISK

**Description:** The amount of free disk is below configured thresholds

**Default Severity:** Major

**OID:** comcolLowDiskFreeNotify

**Recovery:**

1. Remove unnecessary or temporary files from partitions.

2. If there are no files known to be unneeded, contact *My Oracle Support (MOS)*.

## 31118 - DB Disk Store Fault

**Alarm Type:** DISK

**Description:** Writing the database to disk failed

**Default Severity:** Minor

**OID:** comcolDbDiskStoreFaultNotify

**Recovery:**

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact *My Oracle Support (MOS)*.
3. When configuring/reconfiguration a system, changing the NTP server and/or the OAM IP from initial configuration screen in platcfg without stopping the Policy application and COMCOL can cause this alarm. Resolution: Mark standby CMP cluster as "force-standby", and clear the COMCOL database to solve this issue. To avoid this alarm while changing the NTP server and/or OAM IP(s) is to:
   a) Stop qp_procmgr and COMCOL services
   b) Perform the NTP server / OAM IP change
   c) Restart qp_procmgr and COMCOL services

## 31119 - DB Updatelog Overrun

**Alarm Type:** DB

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

**Default Severity:** Minor

**OID:** comcolDbUpdateLogOverrunNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 31120 - DB Updatelog Write Fault

**Alarm Type:** DB

**Description:** A DB change cannot be stored in the updatelog

**Default Severity:** Minor

**OID:** comcolDbUpdateLogWriteFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31121 - Low Disk Free Early Warning

**Alarm Type:** DISK

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

**Default Severity:** Minor

**OID:** comcolLowDiskFreeEarlyWarningNotify

**Recovery:**

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

### 31122 - Excessive Shared Memory Early Warning

**Alarm Type:** MEM

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

**Default Severity:** Minor

**OID:** comcolExcessiveSharedMemoryConsumptionEarlyWarnNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31123 - ADIC Complete

**Alarm Type:** REPL

**Description:** ADIC found one or more errors that are not automatically fixable.

**Default Severity:** Info

**OID:** comcolDbRepAuditCompleteNotify

**Recovery:**

No action required.

### 31124 - ADIC Error

**Alarm Type:** REPL

**Description:** An ADIC detected errors.

**Default Severity:** Minor

**OID:** comcolDbRepAuditCmdErrNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31125 - DB Durability Degraded

**Alarm Type:** REPL

**Description:** DB durability has dropped below configured durability level

**Default Severity:** Major

**OID:** comcolDbDurabilityDegradedNotify

**Recovery:**

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

### 31126 - Audit Blocked

**Alarm Type:** REPL

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

**Default Severity:** Major

**OID:** comcolAuditBlockedNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31127 - DB Replication Audit Complete

**Alarm Type:** REPL

**Description:** DB replication audit completed.

**Default Severity:** Info

**OID:** comcolDbRepAuditComplete

**Recovery:**

No action required.

### 31128 - ADIC Found Error

**Alarm Type:** REPL

**Description:** ADIC found one or more errors that are not automatically fixable.

**Default Severity:** Major

**OID:** comcolDbADICError

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31129 - ADIC Found Minor Issue

**Alarm Type:** REPL

**Description:** ADIC found one or more minor issues that can most likely be ignored.

**Severity:** Minor

**HA Score:** Normal

**Auto Clear Seconds:** 14400

**OID:** comcolDbADICWarn

**Recovery:**

No action required.

### 31130 - Network Health Warning

**Alarm Type:** NET

**Description:** Network health issue detected

**Default Severity:** Minor

**OID:** comcolNetworkHealthWarningNotify

**Recovery:**

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

### 31131 - DB Ousted Throttle Behind

**Alarm Type:** DB

**Description:** DB ousted throttle may be affecting processes.

**Severity:** Minor

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** comcolOustedThrottleWarnNotify

**Recovery:**

1.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31140 - DB Perl Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolDbPerlFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31145 - DB SQL Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolDbSQLFaultNotify

**Recovery:**

1. Export event history for the given server, and Imysqld task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31146 - DB Mastership Fault

**Alarm Type:** SW

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

**Default Severity:** Major

**OID:** comcolDbMastershipFaultNotify

**Recovery:**

1. Export event history for the given server.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31147 - DB UpSyncLog Overrun

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolDbUpSyncLogOverrunNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31148 - DB Lock Error Detected

**Alarm Type:** DB

**Description:** DB lock integrity error detected -- The DB service process (idbsvc) has detected an IDB lock-related error caused by another process. The alarm likely indicates a DB lock-related programming error, or it could be a side effect of a process crash.

**Default Severity:** Minor

**OID:** comcolDbLockErrorNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 31200 - Process Management Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolProcMgmtFaultNotify

**Recovery:**

1. Export event history for the given server, all processes.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 31201 - Process Not Running

**Alarm Type:** PROC

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

**Default Severity:** Major

**OID:** comcolProcNotRunningNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 31202 - Unkillable Zombie Process

**Alarm Type:** PROC

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

**Default Severity:** Major

**OID:** comcolProcZombieProcessNotify

**Recovery:**

1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31206 - Process Mgmt Monitoring Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolProcMgmtMonFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31207 - Process Resource Monitoring Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolProcResourceMonFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31208 - IP Port Server Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolPortServerFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31209 - Hostname Lookup Failed

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolHostLookupFailedNotify

**Recovery:**

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

3. When configuring/reconfiguration a system, the Primary Site/Secondary Site fields in Topology Settings are used to identify the site in which this cluster is located. If The default value "Unspecified" is kept unchanged while configuring Topology as Geo-redundant sites, the other servers in topology may raise this alarm. Resolution: Select the correct site for each cluster being configured in Topology Settings.

## 31213 - Process Scheduler Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolProcSchedulerFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 31214 - Scheduled Process Fault

**Alarm Type:** PROC

**Description:** A scheduled process cannot be executed or abnormally terminated

**Default Severity:** Minor

**OID:** comcolScheduleProcessFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 31215 - Process Resources Exceeded

**Alarm Type:** SW

**Description:** A process is consuming excessive system resources

**Default Severity:** Minor

**OID:** comcolProcResourcesExceededFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 31216 - SysMetric Configuration Error

**Alarm Type:** SW

**Description:** A SysMetric Configuration table contains invalid data

**Default Severity:** Minor

**OID:** comcolSysMetricConfigErrorNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31220 - HA Config Monitor Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolHaCfgMonitorFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31221 - HA Alarm Monitor Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolHaAlarmMonitorFaultNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31222 - HA Not Configured

**Alarm Type:** HA

**Description:** High availability is disabled due to system configuration

**Default Severity:** Minor

**OID:** comcolHaNotConfiguredNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31223 - HA Heartbeat Transmit Failure

**Alarm Type:** HA

**Description:** The high availability monitor failed to send heartbeat

**Default Severity:** Major

**OID:** comcolHaHbTransmitFailureNotify

**Recovery:**

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

### 31224 - HA Configuration Error

**Alarm Type:** HA

**Description:** High availability configuration error

**Default Severity:** Major

**OID:** comcolHaCfgErrorNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31225 - HA Service Start Failure

**Alarm Type:** HA

**Description:** The high availability service failed to start

**Default Severity:** Major

**OID:** comcolHaSvcStartFailureNotify

**Recovery:**

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

### 31226 - HA Availability Status Degraded

**Alarm Type:** HA

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

**Default Severity:** Major

**OID:** comcolHaAvailDegradedNotify

**Recovery:**

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

### 31227 - HA Availability Status Failed

**Alarm Type:** HA

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

**Default Severity:** Critical

**OID:** comcolHaAvailFailedNotify

**Recovery:**

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

## 31228 - HA Standby Server Offline

**Alarm Type:** HA

**Description:** HA Standby Server Offline

**Default Severity:** Critical

**OID:** comcolHaStandbyOfflineNotify

**Recovery:**

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

## 31229 - HA Score Changed

**Alarm Type:** HA

**Description:** High availability health score changed

**Default Severity:** Info

**OID:** comcolHaScoreChangeNotify

**Recovery:**

Status message - no action required.

## 31230 - Recent Alarm Processing Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolRecAlarmEvProcFaultNotify

**Recovery:**

1. Export event history for the given server and raclerk task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31231 - Platform Alarm Agent Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolPlatAlarmAgentNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 31232 - HA Late Heartbeat Warning

**Alarm Type:** HA

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

**Default Severity:** Minor

**OID:** comcolHaLateHeartbeatWarningNotify

**Recovery:**

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

### 31233 - HA Secondary Path Down

**Alarm Type:** HA

**Description:** High availability secondary path loss of connectivity

**Default Severity:** Major

**OID:** comcolHaSecPathDown

**Recovery:**

1. If loss of communication between the active and standby servers over the secondary path is caused intentionally by maintenance activity, the 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 and/or contact *My Oracle Support (MOS)*.

### 31234 - Untrusted Time Upon Initialization

**Alarm Type:** SW

**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

**HA Score** : Normal

**Auto Clear Seconds:** 0

**OID:** comcolUtrustedTimeOnInit

**Recovery:**

1. Correct NTP configuration.
2. If required, contact *My Oracle Support (MOS)*.

## 31235 - Untrusted Time After Initialization

**Alarm Type:** SW

**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

**HA Score** : Normal

**Auto Clear Seconds:** 86400

**OID:** comcolUtrustedTimePostInit

**Recovery:**

1. Correct NTP configuration.
2. If required, contact *My Oracle Support (MOS)*.

## 31236 - HA Link Down

**Alarm Group:** HA

**Description:** High availability TCP link is down.

**Severity:** Critical

**Instance:** Remote node being connected to plus the path identifier

**HA Score:** Normal

**Auto Clear Seconds:** 300

**OID:** comcolHaLinkDownNotify

**Recovery:**

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

### 31240 - Measurements Collection Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolMeasCollectorFaultNotify

**Recovery:**

1. Export event history for the given server and statclerk task.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31250 - RE Port Mapping Fault

**Alarm Type:** SW

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

**Default Severity:** Minor

**OID:** comcolRePortMappingFaultNotify

**Recovery:**

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

### 31260 - DB SNMP Agent

**Alarm Type:** SW

**Description:** The DB SNMP agent (snmpIdbAgent) is impaired by a s/w fault

**Default Severity:** Minor

**OID:** comcolDbSnmpAgentNotify

**Recovery:**

1. Export event history for the given server and all processes.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 31270 - Logging Output

**Alarm Type:** SW

**Description:** Logging output set to Above Normal

**Default Severity:** Minor

**OID:** comcolLoggingOutputNotify

**Recovery:**

Extra diagnostic logs are being collected, potentially degrading system performance. If the problem persists, contact *My Oracle Support (MOS)*.

### 31280 - HA Active to Standby Transition

**Alarm Type:** HA

**Description:** HA active to standby activity transition

**Default Severity:** Info

**OID:** comcolActiveToStandbyTransNotify

**Recovery:**

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

### 31281 - HA Standby to Active Transition

**Alarm Type:** HA

**Description:** HA standby to active activity transition

**Default Severity:** Info

**OID:** comcolStandbyToActiveTransNotify

**Recovery:**

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

### 31282 - HA Management Fault

**Alarm Type:** HA

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

**Default Severity:** Minor

**OID:** comcolHaMgmtFaultNotify

**Recovery:**

Export event history for the given server and cmha task, then contact *My Oracle Support (MOS)*.

### 31283 - HA Server Offline

**Alarm Type:** HA

**Description:** High availability server is offline

**Default Severity:** Critical

**OID:** comcolHAServerOfflineNotify

**Recovery**

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

## 31284 - HA Remote Subscriber Heartbeat Warning

**Alarm Type:** HA

**Description:** High availability remote subscriber has not received a heartbeat within the configured interval

**Default Severity:** Minor

**OID:** comcolHARemoteHeartbeatWarningNotify

**Recovery**

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

## 31285 - HA Split Brain Recovery Entry

**Alarm Group:** HA

**Description:** High availability split brain 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 Split Brain Recovery Plan

**Alarm Group:** HA

**Description:** High availability split brain 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 split brain recovery.

## 31287 - HA Split Brain Recovery Complete

**Alarm Group:** HA

**Description:** High availability split brain 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 split brain recovery.

## 31290 - HA Process Status

**Alarm Type:** HA

**Description:** HA manager (cmha) status

**Default Severity:** Info

**OID:** comcolHaProcessStatusNotify

**Recovery:**

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

## 31291 - HA Election Status

**Alarm Type:** HA

**Description:** HA DC Election status

**Default Severity:** Info

**OID:** comcolHAElectionStatusNotify

**Recovery:**

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

### 31292 - HA Policy Status

**Alarm Type:** HA

**Description:** HA Policy plan status

**Default Severity:** Info

**OID:** comcolHaPolicyStatusNotify

**Recovery:**

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

### 31293 - HA Resource Link Status

**Alarm Type:** HA

**Description:** HA Resource Agent Link status

**Default Severity:** Info

**OID:** comcolHaRaLinkStatusNotify

**Recovery:**

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

### 31294 - HA Resource Status

**Alarm Type:** HA

**Description:** HA Resource registration status

**Default Severity:** Info

**OID:** comcolHaResourceStatusNotify

**Recovery:**

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

### 31295 - HA Action Status

**Alarm Type:** HA

**Description:** HA Resource action status

**Default Severity:** Info

**OID:** comcolHaActionStatusNotify

**Recovery:**

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

### 31296 - HA Monitor Status

**Alarm Type:** HA

**Description:** HA Monitor action status

**Default Severity:** Info

**OID:** comcolHaMonitorStatusNotify

**Recovery:**

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

### 31297 - HA Resource Agent Info

**Alarm Type:** HA

**Description:** HA Resource Agent application information

**Default Severity:** Info

**OID:** comcolHaRaInfoNotify

**Recovery:**

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

### 31298 - HA Resource Agent Detail

**Alarm Type:** HA

**Description:** HA Resource Agent application detailed information

**Default Severity:** Info

**OID:** comcolHaRaDetailNotify

**Recovery:**

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

### 31299 - HA Notification Status

**Alarm Type:** HA

**Description:** HA Notification Status

**Default Severity:** Info

**OID:** comcolHaNotification

**Recovery:**

No action required.

## 31300 - HA Control Status

**Alarm Type:** HA

**Description:** HA Control action status

**Default Severity:** Info

**OID:** comcolHaControl

**Recovery:**

No action required.

## 32113 - Uncorrectable ECC Memory Error

**Alarm Type:** PLAT

**Description:** Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

**Default Severity:** Critical

**OID:** tpdEccUncorrectableError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)* to request hardware replacement.

## 32114 - SNMP Get Failure

**Alarm Type:** PLAT

**Description:** SNMP Get Failure -- The server failed to receive SNMP information from the switch.

**Default Severity:** Critical

**OID:** tpdSNMPGetFailure

Within this trap is one bind variable, the OID of which is 1.3.6.1.2.1.1.5 <sysname>, where <sysname> is the name of the switch where the failure occurred.

**Recovery**

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

### 32115 - TPD NTP Daemon Not Synchronized Failure

**Alarm Type:** PLAT

**Description:** This alarm indicates that the server is not synchronized to an NTP source, has not been synchronized for an extended number of hours, and has reached the critical threshold.

**Default Severity:** Critical

**HA Score:** Normal

**OID:** tpdNTPDaemonNotSynchronizedFailure

**Recovery**

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

### 32116 - TPD Server's Time Has Gone Backwards

**Alarm Type:** PLAT

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

**Default Severity:** Critical

**HA Score:** Normal

**OID:** tpdNTPTimeGoneBackwards

**Recovery**

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

### 32117 - TPD NTP Offset Check Failure

**Alarm Type:** PLAT

**Description:** This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold.

**Default Severity:** Critical

**HA Score:** Normal

**OID:** ntpOffsetCheckFailure descr

**Recovery**

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

### 32300 – Server Fan Failure

**Alarm Type:** PLAT

**Description:** Server Fan Failure -- This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

**Default Severity:** Major

**OID:** tpdFanError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32301 - Server Internal Disk Error

**Alarm Type:** PLAT

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

**Default Severity:** Major

**OID:** tpdIntDiskError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32302 – Server RAID Disk Error

**Alarm Type:** PLAT

**Description:** Server RAID Disk Error -- This alarm indicates that the offboard storage server had a problem with its hardware disks.

**Default Severity:** Major

**OID:** tpdRaidDiskError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32303 - Server Platform Error

**Alarm Type:** PLAT

**Description:** Server Platform Error - This alarm indicates an error such as a corrupt system configuration or missing files.

**Default Severity:** Major

**OID:** tpdPlatformError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32304 - Server File System Error

**Alarm Type:** PLAT

**Description:** Server File System Error -- This alarm indicates unsuccessful writing to at least one of the server's file systems.

**Default Severity:** Major

**OID:** tpdFileSystemError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32305 - Server Platform Process Error

**Alarm Type:** PLAT

**Description:** Server Platform Process Error -- This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

**Default Severity:** Major

**OID:** tpdPlatProcessError

**Recovery**

If the problems persists, contact *My Oracle Support (MOS)*.

## 32307 - Server Swap Space Shortage Error

**Alarm Type:** PLAT

**Description:** Server Swap Space Shortage Error -- This alarm indicates that the server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.

**Default Severity:** Major

**OID:** tpdSwapSpaceShortageError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32308 - Server Provisioning Network Error

**Alarm Type:** PLAT

**Description:** Server Provisioning Network Error -- This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly. The eth1 interface is at the upper right port on the rear of the server on the EAGLE backplane.

**Default Severity:** Major

**OID:** tpdProvNetworkError

**Recovery**

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

## 32312 - Server Disk Space Shortage Error

**Alarm Type:** PLAT

**Description:** Server Disk Space Shortage Error -- This alarm indicates that one of the following conditions has occurred:

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

**Default Severity:** Major

**OID:** tpdDiskSpaceShortageError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32313 - Server Default Route Network Error

**Alarm Type:** PLAT

**Description:** Server Default Route Network Error -- This alarm indicates that the default network route of the server is experiencing a problem.


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

**Default Severity:** Major

**OID:** tpdDefaultRouteNetworkError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32314 - Server Temperature Error

**Alarm Type:** PLAT

**Description:** Server Temperature Error -- The internal temperature within the server is unacceptably high.

**Default Severity:** Major

**OID:** tpdTemperatureError

**Recovery**

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

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

3. If the problem has not been resolved, contact *My Oracle Support (MOS)*.

## 32315 – Server Mainboard Voltage Error

**Alarm Type:** PLAT

**Description:** Server Mainboard Voltage Error -- This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.

**Default Severity:** Major

**OID:** tpdServerMainboardVoltageError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32316 – Server Power Feed Error

**Alarm Type:** PLAT

**Description:** Server Power Feed Error -- This alarm indicates that one of the power feeds to the server has failed. If this alarm occurs in conjunction with any Breaker Panel alarm, there might be a problem with the breaker panel.

**Default Severity:** Major

**OID:** tpdPowerFeedError

**Recovery**

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

## 32317 - Server Disk Health Test Error

**Alarm Type:** PLAT

**Description:** Server Disk Health Test Error -- Either the hard drive has failed or failure is imminent.

**Default Severity:** Major

**OID:** tpdDiskHealthError

**Recovery**

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

## 32318 - Server Disk Unavailable Error

**Alarm Type:** PLAT

**Description:** Server Disk Unavailable Error -- The `smartd` service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

**Default Severity:** Major

**OID:** tpdDiskUnavailableError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32320 – Device Interface Error

**Alarm Type:** PLAT

**Description:** Device Interface Error -- This alarm indicates that the IP bond is either not configured or down.

**Default Severity:** Major

**OID:** tpdDeviceIfError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32321 – Correctable ECC memory error

**Alarm Type:** PLAT

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

**Default Severity:** Major

**OID:** tpdEccCorrectableError

**Recovery**

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

### 32322 – Power Supply A error

**Alarm Type:** PLAT

**Description:** Power Supply A Error -- This alarm indicates that power supply 1 (feed A) has failed.

**Default Severity:** Major

**OID:** tpdPowerSupply1Error

**Recovery**

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

### 32323 – Power Supply B Error

**Alarm Type:** PLAT

**Description:** Power Supply B Error -- This alarm indicates that power supply 2 (feed B) has failed.

**Default Severity:** Major

**OID:** tpdPowerSupply2Error

**Recovery**

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

## 32324 – Breaker panel Feed Error

**Alarm Type:** PLAT

**Description:** Breaker Panel Feed Error -- This alarm indicates that the server is not receiving information from the breaker panel relays.

**Default Severity:** Major

**OID:** tpdBrkPnlFeedError

**Recovery**

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

## 32325 – Breaker Panel Breaker Error

**Alarm Type:** PLAT

**Description:** Breaker Panel Breaker Error -- This alarm indicates that a power fault has been identified by the breaker panel.

**Default Severity:** Major

**OID:** tpdBrkPnlBreakerError

**Recovery**

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

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

a) For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.

b) After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, contact *My Oracle Support (MOS)*.

- If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, continue with the next step.

4. If the problem has not been resolved, contact *My Oracle Support (MOS)*.

## 32326 – Breaker Panel Monitoring Error

**Alarm Type:** PLAT

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

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

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

until the Breaker Panel Monitoring Error has been corrected.

**Default Severity:** Major

**OID:** tpdBrkPnlMntError

**Recovery**

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

## 32327 – Server HA Keepalive Error

**Alarm Type:** PLAT

**Description:** Server HA Keepalive Error -- This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

**Default Severity:** Major

**OID:** tpdHaKeepaliveError

**Recovery**

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

   **Note:** This step may require command line ability.

4. If the problem persists, contact *My Oracle Support (MOS)*.

## 32331 – HP disk problem

**Alarm Type:** TPD

**Description:** HP disk problem -- This major alarm indicates that there is an issue with either a physical or logical disk in the HP disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.

**Default Severity:** Major

**OID:** tpdHpDiskProblemNotify

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32332 – HP Smart Array controller problem

**Alarm Type:** PLAT

**Description:** HP Smart Array controller problem -- This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.

**Default Severity:** Major

**OID:** tpdHpDiskCtrlrProblemNotify

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32333 – HP hpacucliStatus utility problem

**Alarm Type:** PLAT

**Description:** HP hpacucliStatus utility problem -- This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus/hpDiskStatus daemon is either not running, or hung.

**Default Severity:** Major

**OID:** tpdHPACUCLIProblem

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32335 - Switch Link Down Error

**Alarm Type:** PLAT

**Description:** Swith Link Down Error -- The link is down.

**Default Severity:** Major

**OID:** tpdSwitchLinkDownError

Within this trap are two bind variables, the OIDs of which are:

- 1.3.6.1.2.1.1.5 <sysname>, where <sysname> is the name of the switch where the failure occurred.
- 1.3.6.1.2.1.2.2.1.1 <link index>, where <link index> is the index of the failed link.

**Recovery**

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

## 32336 – Half open socket limit

**Alarm Type:** PLAT

**Description:** Half open socket limit -- This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

**Default Severity:** Major

**OID:** tpdHalfOpenSockLimit

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32339 - TPD Max Number Of Running Processes Error

**Alarm Type:** PLAT

**Description:** This alarm indicates that the maximum number of running processes has reached the major threshold.

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdMaxPidLimit

**Recovery**

1. Run syscheck in verbose mode.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 32340 - TPD NTP Daemon Not Synchronized Error

**Alarm Type:** PLAT

**Description:** This alarm indicates that the server is not synchronized to an NTP source, has not been synchronized for an extended number of hours, and has reached the major threshold.

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdNTPDaemonNotSynchronizedError

**Recovery**

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

### 32341 - TPD NTP Daemon Never Synchronized Error

**Alarm Type:** 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.

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdNTPDaemonNeverSynchronized

**Recovery**

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

### 32342 - TPD NTP Offset Check Error

**Alarm Type:** PLAT

**Description:** This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.

**Default Severity:** Major

**HA Score:** Normal

**OID:** ntpOffsetCheckError

**Recovery**

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

## 32343 - TPD RAID disk problem

**Alarm Type:** PLAT

**Description:** This alarm indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdDiskProblem

**Recovery**

1. Run syscheck in verbose mode.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 32344 - RAID controller problem

**Alarm Type:** PLAT

**Description:** This alarm indicates that RAID controller needs intervention. State reported by syscheck is not "Normal" and/or BBU (backup battery unit) state is not "Operational."

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdDiskCtrlrProblem

**Recovery**

1. Run syscheck in verbose mode.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 32345 - Server Upgrade snapshot(s) invalid

**Alarm Type:** PLAT

**Description:** This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible.

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdUpgradeSnapshotInvalid

**Recovery**

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

### 32346 - OEM hardware management service reports an error

**Alarm Type:** PLAT

**Description:** This alarm indicates that OEM hardware management service reports an error.

**Default Severity:** Major

**HA Score:** Normal

**OID:** tpdOEMHardwareProblem

**Recovery**

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

### 32347 - The hwmgmtcliStatus daemon needs intervention

**Alarm Type:** PLAT

**Description:** This alarm indicates the hwmgmtcliStatus daemon is not running or is not responding.

**Default Severity:** Major

**OID:** tpdHWMGMTCLIProblem

**Recovery**

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

### 32500 – Server Disk Space Shortage Warning

**Alarm Type:** PLAT

**Description:** Server Disk Space Shortage Warning -- This alarm indicates that one of the following conditions has occurred:

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

**Default Severity:** Minor

**OID:** tpdDiskSpaceShortageWarning

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32501 – Server Application Process Error

**Alarm Type:** PLAT

**Description:** Server Application Process Error -- This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

**Default Severity:** Minor

**OID:** tpdApplicationProcessError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32502 – Server Hardware Configuration Error

**Alarm Type:** PLAT

**Description:** Server Hardware Configuration Error -- This alarm indicates that one or more of the server's hardware components are not in compliance with required specifications (refer to the appropriate hardware manual).

**Default Severity:** Minor

**OID:** tpdHardwareConfigError

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32505 – Server Swap Space Shortage Warning

**Alarm Type:** PLAT

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

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

**Default Severity:** Minor

**OID:** tpdSwapSpaceShortageWarning

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32506 – Server Default Router not Defined

**Alarm Type:** PLAT

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

**Default Severity:** Minor

**OID:** tpdDefaultRouteNotDefined

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32507 – Server Temperature Warning

**Alarm Type:** PLAT

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

**Default Severity:** Minor

**OID:** tpdTemperatureWarning

**Recovery**

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

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

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

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

4. If the problem has not been resolved, contact *My Oracle Support (MOS)*.

## 32508 – Server Core File Detected

**Alarm Type:** PLAT

**Description:** Server Core File Detected -- This alarm indicates that an application process has failed and debug information is available.

**Default Severity:** Minor

**OID:** tpdCoreFileDetected

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32509 – Server NTP Daemon Not Synchronized

**Alarm Type:** PLAT

**Description:** Server NTP Daemon Not Synchronized -- This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

**Default Severity:** Minor

**OID:** tpdNTPDeamonNotSynchronized

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32510 – CMOS Battery Voltage Low

**Alarm Type:** PLAT

**Description:** CMOS Battery Voltage Low -- The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.

**Default Severity:** Minor

**OID:** tpdCMOSBatteryVoltageLow

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32511 – Server Disk Self Test Warning

**Alarm Type:** PLAT

**Description:** Server Disk Self Test Warning -- A non-fatal disk issue (such as a sector cannot be read) exists.

**Default Severity:** Minor

**OID:** tpdSmartTestWarn

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32512 – Device Warning

**Alarm Type:** PLAT

**Description:** Device Warning -- This alarm indicates that either we are unable to perform an snmpget command on the configured SNMP OID or the value returned failed the specified comparison operation.

**Default Severity:** Minor

**OID:** tpdDeviceWarn

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32513 – Device Interface Warning

**Alarm Type:** PLAT

**Description:** Device Interface Warning -- This alarm can be generated by either an SNMP trap or an IP bond error.

**Default Severity:** Minor

**OID:** tpdDeviceIfWarn

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32514 – Server Reboot Watchdog Initiated

**Alarm Type:** PLAT

**Description:** Server Reboot Watchdog Initiated -- This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.

**Default Severity:** Minor

**OID:** tpdWatchdogReboot

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32515 – Server HA Failover Inhibited

**Alarm Type:** PLAT

**Description:** Server HA Failover Inhibited -- This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.

**Default Severity:** Minor

**OID:** tpdHaInhibited

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32516 – Server HA Active To Standby Transition

**Alarm Type:** PLAT

**Description:** Server HA Active To Standby Transition -- This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

**Default Severity:** Minor

**OID:** tpdHaActiveToStandbyTrans

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32517 – Server HA Standby To Active Transition

**Alarm Type:** PLAT

**Description:** Server HA Standby To Active Transition -- This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

**Default Severity:** Minor

**OID:** tpdHaStandbyToActiveTrans

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32518 – Platform Health Check Failure

**Alarm Type:** PLAT

**Description:** Platform Health Check Failure -- This alarm is used to indicate a configuration error.

**Default Severity:** Minor

**OID:** tpdHealthCheckFailed

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32519 – NTP Offset Check Failure

**Alarm Type:** PLAT

**Description:** NTP Offset Check Failure -- This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the NTP server and the offset limit that the application has set for the system.

**Default Severity:** Minor

**OID:** ntpOffsetCheckFailed

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

### 32520 – NTP Stratum Check Failure

**Alarm Type:** PLAT

**Description:** NTP Stratum Check Failure -- This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

**Default Severity:** Minor

**OID:** ntpStratumCheckFailed

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32521 – SAS Presence Sensor Missing

**Alarm Type:** PLAT

**Description:** SAS Presence Sensor Missing -- This alarm indicates that the T1200 server drive sensor is not working.

**Default Severity:** Minor

**OID:** sasPresenceSensorMissing

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)* to get a replacement server.

## 32522 – SAS Drive Missing

**Alarm Type:** PLAT

**Description:** SAS Drive Missing -- This alarm indicates that the number of drives configured for this server is not being detected.

**Default Severity:** Minor

**OID:** sasDriveMissing

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)* to determine whether the issue is with a failed drive or failed configuration.

## 32524 – HP disk resync

**Alarm Type:** PLAT

**Description:** HP disk resync -- This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependant on the size of the disk and the amount of activity on the system.

**Default Severity:** Minor

**OID:** tpdHpDiskResync

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32525 – Telco Fan Warning

**Alarm Type:** PLAT

**Description:** Telco Fan Warning -- This alarm indicates that the Telco switch has detected an issue with an internal fan.

**Default Severity:** Minor

**OID:** tpdTelcoFanWarning

**Recovery**

1. If the problem persists, contact *My Oracle Support (MOS)* to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.
2. *My Oracle Support (MOS)* personnel can perform an snmpget command or log into the switch to get detailed fan status information.

## 32526 – Telco Temperature Warning

**Alarm Type:** PLAT

**Description:** Telco Temperature Warning -- This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.

**Default Severity:** Minor

**OID:** tpdTelcoTemperatureWarning

**Recovery**

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

## 32527 – Telco Power Supply Warning

**Alarm Type:** PLAT

**Description:** Telco Power Supply Warning -- This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

**Default Severity:** Minor

**OID:** tpdTelcoPowerSupplyWarning

**Recovery**

1. Verify breaker wasn't tripped.
2. If breaker is still good and problem persists, contact *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 Type:** PLAT

**Description:** Invalid BIOS value -- This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.

**Default Severity:** Minor

**OID:** tpdInvalidBiosValue

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32529 – Server Kernel Dump File Detected

**Alarm Type:** PLAT

**Description:** Server Kernel Dump File Detected -- This alarm indicates that the kernel has crashed and debug information is available.

**Default Severity:** Minor

**OID:** tpdServerKernelDumpFileDetected

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32530 – TPD Upgrade Fail Detected

**Alarm Type:** PLAT

**Description:** Server Upgrade Fail Detected -- This alarm indicates that a TPD upgrade has failed.

**Default Severity:** Minor

**OID:** tpdUpgradeFailed

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32531 – Half Open Socket Warning

**Alarm Type:** PLAT

**Description:** Half Open Socket Warning -- This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

**Default Severity:** Minor

**OID:** tpdHalfOpenSocketWarning

**Recovery**

If the problem persists, contact *My Oracle Support (MOS)*.

## 32532 – Server Upgrade Pending Accept/Reject

**Alarm Type:** PLAT

**Description:** Server Upgrade Pending Accept/Reject -- This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

**Default Severity:** Minor

**OID:** tpdServerUpgradePendingAccept

**Recovery**

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

## 32533 -TPD Max Number Of Running Processes Warning

**Alarm Type:** PLAT

**Description:** This alarm indicates that the maximum number of running processes has reached the minor threshold.

**Default Severity:** Minor

**OID:** tpdMaxPidWarning

**Recovery**

1. Run syscheck in verbose mode.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 32534 -TPD NTP Source Is Bad Warning

**Alarm Type:** 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.

**Default Severity:** Minor

**OID:** tpdNTPSourceIsBad

**Recovery**

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

## 32535 -TPD RAID disk resync

**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 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).

**Default Severity:** Minor

**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)*.

### 32536 - Server Upgrade Snapshot(s) warning

**Alarm Type:** 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 100% full and invalid.

**Default Severity:** Minor

**OID:** tpdUpgradeSnapshotWarning

**Recovery**

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

## QBus Platform (70000-70999)

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

### 70001 - QP_procmgr failed

**Alarm Type:** QP

**Description:** The QP-procmgr process has failed. This process manages all pcrf software.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Failed

**Clearing Action:** This alarm is cleared by qp-procmgr after qp-procmgr is restarted.

**OID:** pcrfMIBNotificationsQPProcmgrFailedNotify

**Recovery:**

If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact *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 is cleared automatically.

**OID:**pcrfMIBNotificationsQPCriticalProcFailedNotify

**Recovery:**

This alarm automatically clears as Policy processes are restarted. If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact *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:** pcrfMIBNotificationsQPNonCriticalProcFailedNotify

**Recovery:**

If the alarm occurs infrequently, monitor the health of the system. 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:** pcrfMIBNotificationsQPMaintShutdownNotify

**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:**pcrfMIBNotificationsQPClusterStatusNotify

**Recovery:**

If the alarm occurs infrequently, monitor the health of the system. If the alarm occurs frequently, contact *My Oracle Support (MOS)*.

## Error Code Details for Alarms 70010 and 70011

**Table 5: Error Code and Meaning - Alarms 70010/70011**

| Error Code | Meaning |
|---|---|
| 1 | Syntax or usage error |
| 2 | Protocol incompatibility |
| 3 | Errors selecting input/output files, dirs |
| 4 | Requested action not supported: an attempt was made to manipulate 64-bit files on a platform that cannot support them; or an option was specified that is supported by the client and not by the server |
| 5 | Error starting client-server protocol |
| 6 | Daemon unable to append to log-file |
| 10 | Error in socket I/O |
| 11 | Error in file I/O |
| 12 | Error in rsync protocol data stream |
| 13 | Errors with program diagnostics |
| 14 | Error in IPC code |
| 20 | Received SIGUSR1 or SIGINT |
| 21 | Some error returned by waitpid() |
| 22 | Error allocating core memory buffers |

| Error Code | Meaning |
|---|---|
| 23 | Partial transfer due to error |
| 24 | Partial transfer due to vanished source files |
| 25 | The --max-delete limit stopped deletions 30 Timeout in data send/receive |
| 101 | No mate found. Blade may be in degraded state |
| 102 | Called from master with '--fromMaster' option |
| 103 | Incorrect usage |
| 104 | Failed in key exchange with remote host |

## 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>
- 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.

**OID:** pcrfMIBNotificationsQPServerBackupRsyncFailedNotify

**Recovery:**

Check that the parameters are correct. Take corrective action based on the returned *Error Code Details for Alarms 70010 and 70011*.

## 70011 - QP Failed System-backup Remote Archive Rsync

**Alarm Type:** QP

**Description:** A scheduled backup failed to synchronize the local system-backup archive with the remote system-backup archive.

Hostname=<hostname | IPaddr>, user=<user>, path=<path>,errorcode=<rsync error>

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 64800 seconds.

**OID:** pcrfMIBNotificationsQPSystemBackupRsyncFailedNotify

**Recovery:**

Check that the parameters are correct. Take corrective action based on the returned *Error Code Details for Alarms 70010 and 70011*.

## 70012 - QP Failed To Create Server Backup

**Alarm Type:** QP

**Description:** A scheduled backup failed to create the local server-backup file.

Failure-reason=<errorcode>

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 64800 seconds.

**OID:** pcrfMIBNotificationsQPServerBackupFailedNotify

**Recovery:**

Take corrective action based on the returned error message.

## 70013 - QP Failed To Create System Backup

**Alarm Type:** QP

**Description:** A scheduled backup failed to create the local system-backup file.

Failure-reason=<errorcode>

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 64800 seconds.

**OID:** pcrfMIBNotificationsQPSystemBackupFailedNotify

**Recovery:**

Take corrective action based on the returned error message.

## 70015 - VIP Route Add Failed

**Alarm Type:** QP

**Description:** VIP Route Add Failed -- VIP route add failed to re-apply during VIP event.

The alarm displays the following information:

- IP-Type

- Route-Type
- Network
- Destination
- Gateway-Address
- Error Message

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 3600 seconds.

**OID:** pcrfMIBNotificationsQpAddRouteFailedNotify

**Recovery:**

Use server UI (Platcfg Routing Menu) to repair the route manually.

## 70020 - QP Master database is outdated

**Alarm Type:** QP

**Description:** The current MYSQL master server has an outdated database.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Degraded

**Clearing Action:** This alarm clears when the master server either is made a slave server or if a database restore action clears the condition.

**OID:** pcrfMIBNotificationsQPMySQLMasterOutdatedNotify

**Recovery:**

1. Once the condition has occurred, the 80003 event will be sent once a minute. Wait until all of the expected servers are being reported. It is important to wait because the best slave might be undergoing a reboot and its DB Level will not be known until after the reboot completes.
2. Use the information in 80003 to select the new master candidate.
3. Except for the current master and the master candidate, put all of the other servers into forcedStandby.
4. If the best slave is in the same cluster (the most common case), simply perform a failover by restarting the current active blade. If the best slave is in a separate cluster, then a site promotion is necessary.
5. Remove the forced standby settings on the other slaves.
6. If none of the slaves are good candidates, perform a database restore.
   a) Put all of the slave servers into forced standby state
   b) Perform a restore on the active server.
      The restore will clear the condition.
   c) Take the slave servers out of the standby state.

### 70021 - QP slave database is unconnected to the master

**Alarm Type:** QP

**Description:** The MySQL slave is not connected to the master.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Failed

**Clearing Action:** This alarm clears automatically when the slave server connects to the master server.

**OID:**pcrfMIBNotificationsQPMySQLSlaveUnconnectedNotify

**Recovery:**

1. No action required unless the alarm does not clear within a few hours.
2. If the problem persists, contact *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:** pcrfMIBNotificationsQPMySQLSlaveSyncFailureNotify

**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:** pcrfMIBNotificationsQPMySQLSlaveLaggingNotify

**Recovery:**

1. No action required unless the alarm does not clear within a few hours or the condition is repeatedly set and unset.
2. If either of the problems persists, contact *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 sychronizing with the master -- The MySQL slave database has been prevented from synchronization with the master database because the master database is outdated.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Degraded

**Clearing Action:** This alarm clears when the slave database is synchronized with the master database. This alarm is set on the slave server and will only occur when the active server on the primary site has set alarm 70020. This alarm clears automatically when the slave database is synchronized with the master database.

**OID:**pcrfMIBNotificationsQPMySQLSlaveSyncPreventedNotify

**Recovery:**

1. Diagnose the CMP master server to clear its 70020 alarm.
2. Once alarm 70020 is cleared, the slave server will clear alarm 70024.

## 70025 - QP Slave database is a different version than the master

**Alarm Type:** QP

**Description:**The MySQL slave has a different schema version than the master.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** DegradedNormal

**Clearing Action:** The slave server clears the alarm when the master DB version is equal to the slave DB version.

**OID:**pcrfMIBNotificationsQPMySQLSchemaVersionMismatchNotify

**Recovery:**

This alarm is set by the CMP Slave Server during a CMP Server Upgrade or Backout, when the CMP Master Server DB is a different version than the CMP Slave Server DB. The Slave Server clears the alarm when the Master Server and the Slave Server again have the same version.

### 70026 - QP Server Symantec NetBackup Operation in Progress

**Alarm Type:** QP

**Description:** Server is performing a Symantec NetBackup Operation.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Alarm clears when the NetBackup client operation has completed.

**OID:** pcrfMIBNotificationsQPNetBackupInProgressNotify

**Recovery:**

1. When operation is complete, alarm should clear.
2. If the alarm does not clear within a few hours, then check the NetBackup Server logs.
3. If the NetBackup Server logs have no errors, or if the alarm is occurring over and over, contact *My Oracle Support (MOS)*.

### 70028 - QP Signaling Bonded Interface is Down

**Alarm Type:** QP

**Description:** Indicates both bond interfaces SIGA and SIGB are disconnected, and a failover has occurred. The cluster status changes to Degraded.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Degraded

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPSignalBondedInterfaceDownNotify

**Recovery:**

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

### 70029 - QP Peer Node Bonded Interface is Down

**Alarm Type:** QP

**Description:** Indicates QP peer node bonded interface is down.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPPeerBondedInterfaceDown

**Recovery:**

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

## 70030 - QP Backplane Bonded Interface is Down

**Alarm Type:** QP

**Description:** Indicates Backplane bonded interface bond3 is down.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPBackplaneBondedInterfaceDown

**Recovery:**

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

## 70031 - QP degrade because one or more interfaces are down

**Alarm Type:** QP

**Description:** QP degrade because one or more interfaces are down

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPInterfacesDegradeNotify

**Recovery:**

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

## 70032 - QP direct link does not work as configuration

**Alarm Type:** QP

**Description:** QP degrade because one or more interfaces are down

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPBpMismatchNotify

**Recovery:**

1. This alarm is due to the incorrect configuration of backplane so that it cannot be applied to the system. Check the validity of backplane IP Address and Comcol table LogicPath.

## 70050 - QP Timezone Change Detected

**Alarm Type:** QP

**Description:** Timezone has been changed using platcfg. Application needs to be restarted.

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

## 70500 - Upgrade Director System Mixed Version

**Alarm Type:** QP

**Description:** There are multiple software versions running in the system because of an upgrade or backout.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsSystemMixedVersionNotify

**Recovery:**

1. 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. 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 - Upgrade Director 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 (e.g. loss of redundancy/replication). Certain operations may not be possible for the cluster while this alarm is asserted.

**Default Severity:** Minor

**Instance:** The Comcol ID of the cluster.

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsClusterMixedVersionNotify

**Recovery:**

1. 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. 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 - Upgrade Director 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 hostname of the server.

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsClusterReplicationInhibitedNotify

**Recovery:**

1. This alarm is raised when the upgrade director determines that replication should be inhibited to a server. Once the server completes upgrade/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- Upgrade Director 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:** pcrfMIBNotificationsServerForcedStandbyNotify

**Recovery:**

1. This alarm is raised when the upgrade director determines a server is not running the same version of software as the active server in the cluster. When this server completes upgrade/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)*.

## 70504 - Upgrade Director Upgrade Tool Mismatch

**Alarm Type:** UD

**Description:** This server is not running with the expected set of upgrade tools.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This is not an auto-clear alarm.

**OID:**

**Recovery:**

1. If the alarm does not clear automatically, contact *My Oracle Support (MOS)*.

## 70505 - Upgrade Director ISO Mismatch

**Alarm Type:** QP

**Description:** 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 (e.g. the wrong version).

**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:** pcrfMIBNotificationsISOMismatchNotify

**Recovery:**

1. Currently N/A because this alarm is a placeholder and is not currently active. When it does become active, the solution will be to have the operator remove the offending ISO from /var/TKLC/log on the afflicted machine.
2. If the alarm does not clear automatically, contact *My Oracle Support (MOS)*.

## 70506 - Upgrade Director Operation Failed

**Alarm Type:** QP

**Description:** An action initiated by the upgrade director has failed.

**Default Severity:** Minor

**Instance:** The Comcol ID of the server. Note the alarm text will contain the proper hostname of the server.

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsUpgradeOperationFailedNotify

**Recovery:**

1. If the alarm does not clear automatically, contact *My Oracle Support (MOS)*.

## 70507 - Upgrade Director In Progress

**Alarm Type:** QP

**Description:** An upgrade/backout is in progress for the specified server.

**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:** pcrfMIBNotificationsUpgradeInProgressNotify

**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 - Upgrade Director Server Is Zombie

**Alarm Type:** QP

**Description:** A server has failed an upgrade/backout and now is in an unknown state.

**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:** pcrfMIBNotificationsServerIsZombieNotify

**Recovery:**

1. If the alarm does not clear automatically, contact *My Oracle Support (MOS)*.

## Policy Server (71000-89999)

This section provides a list of Policy Server alarms (71000-79999) and events (80000-89999) which are generated by servers such as MPEs and MRAs.

### 71004 - AM CONN LOST

**Alarm Type:** PCRF

**Description:** AM socket closed.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** AM connection restored to remote peer.

**OID:** pcrfMIBNotificationsAMConnLostNotify

**Recovery:**

1. Check the availability of the AM.
2. Check the AM log for a recent failover or other operations that can interrupt communications.
3. If the AM has not failed, make sure that the path from the AM to the MPE device (port 3918) is operational.
4. If the problem persists, contact *My Oracle Support (MOS)*.

### 71101 - DQOS DOWNSTREAM CONNECTION CLOSED

**Alarm Type:**PCRF

**Description:** DQoS Downstream connection is closed.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** DQOS connection restored to a remote peer.

**OID:** pcrfMIBNotificationsDqosDownstreamConnectionClosedNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 71102 - MSC CONN LOST

**Alarm Type:** PCRF

**Description:** MSC Conn Lost -- The connection was lost to the specified CMTS or downstream policy server.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Connection to a remote peer is restored.

**OID:** pcrfMIBNotificationsMSCConnLostNotify

**Recovery:**

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (port 3918) is operational.
4. If the problem persists, contact *My Oracle Support (MOS)*.

## 71103 - PCMM CONN LOST

**Alarm Type:** PCRF

**Description:** PCMM Conn Lost -- The connection was lost to the specified CMTS or downstream policy server.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Connection to a remote peer is restored.

**OID:** pcrfMIBNotificationsPCMMConnLostNotify

**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:** pcrfMIBNotificationsDqosAmConnectionClosedNotify

**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:** pcrfMIBNotificationsSPCConnClosedNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 71402 - TRANSPORT CLOSED

**Alarm Type:** PCRF

**Description:** Diameter Transport Closed -- 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:** pcrfMIBNotificationsTransportClosedNotify

**Recovery:**

1. Check the configuration and availability of the network element.

2. Check the network element for a reboot or other service interruption.
3. If the network element has not failed, ensure the network path from the device to the network element is operational.
4. If the problem persists, contact *My Oracle Support (MOS)*.

## 71403 - TRANSPORT DISCONNECTED

**Alarm Type:** PCRF

**Description:** Diameter Transport Disconnected -- 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:** pcrfMIBNotificationsTransportDisconnectedNotify

**Recovery:**

1. Check the configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the network element has not failed, ensure the network path from the device to the network element is operational.
4. If the problem persists, contact *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 tab of the policy server tab in the CMP GUI.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 300 seconds.

**OID:** pcrfMIBNotificationsDIAMETERNewConnRejectedNotify

**Recovery:**

1. Check the peer configuration and ensure that the peer sees a valid connection with the device.

2. If the problem persists, contact *My Oracle Support (MOS)*.

## 71414 - SCTP PATH STATUS CHANGED

**Alarm Type:** PCRF

**Description:** SCTP Path Status Changed -- Occurs when an MPE or MRA is multihoming. The alarm occurs when one path fails, and clears when the path becomes available again. If the path that is currently transmitting diameter messages fails, the alarm is triggered when the SCTP association tries to send the next diameter message. If the path is not transmitting diameter messages (it is a backup) then it may take up to 30 seconds for the alarm to be triggered, since heartbeat chunks are sent every 30 seconds.

**Default Severity:** Minor

**Instance:** Peer address + Association ID

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 7200 seconds.

**OID:** pcrfMIBNotificationsSctpPathStatusChangedNotify

**Recovery:**

If the problem persists, contact *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.

**OID:** pcrfMIBNotificationsLdapConnFailedNotify

**Recovery:**

Verify that there is no problem with the LDAP server or the network path used to reach the server. If the problem persists, contact *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:** pcrfMIBNotificationsDHCPUnexpectedEventIdNotify

**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:** pcrfMIBNotificationsDHCPUnableToBindEventIdNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. 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:** pcrfMIBNotificationsDHCPResponseTimeoutEventIdNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact *My Oracle Support (MOS)*.

## 71633 - BAD RELAY ADDRESS EVENT ID

**Alarm Type:** PCRF

**Description:** DHCP bad relay address event id.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 30 seconds.

**OID:** pcrfMIBNotificationsDHCPBadRelayAddressEventIdNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact *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:** pcrfMIBNotificationsDHCPBadPrimaryAddressEventIdNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. 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:** pcrfMIBNotificationsDHCPBadSecondaryAddressEventIdNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. 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:** pcrfMIBNotificationsSPRConnectionClosedNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 71685 - MSR DB NOT REACHABLE

**Alarm Type:** PCRF

**Description:** Unable to connect to MSR after several attempts.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Connection to MSR is restored.

**OID:** pcrfMIBNotificationsMSRDBNotReachableNotify

**Recovery:**

Verify that there is no problem with the MSR server or the network path used to reach the server. If the problem persists, contact *My Oracle Support (MOS)*.

## 71702 - BRAS CONNECTION CLOSED

**Alarm Type:** PCRF

**Description:** Bras Connection Closed -- The MPE lost a connection to the B-RAS element of the gateway.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Connection to BRAS is restored.

**OID:** pcrfMIBNotificationsBrasConnectionClosedNotify

**Recovery:**

1. Check availability of the gateway.
2. If the gateway has not failed, make sure that the path from the gateway to the MPE is operational.
3. If the problem persists, contact *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.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** COPS network element is associated with MPE.

**OID:** pcrfMIBNotificationsCOPSUnknownGatewayNotify

**Recovery:**

1. Check the configuration of the network elements in the CMP. There should be a B-RAS network element for this gateway and that B-RAS must be associated with this MPE.
   Make sure that the configuration of the B-RAS network element is consistent with the provisioned information on the gateway. The network element name in the CMP must match the provisioned router name on the gateway.
2. If the problem persists, contact *My Oracle Support (MOS)*.

## 71801 - PCMM NO PCEF

**Alarm Type:** PCRF

**Description:** No PCEF available for subscriber IP.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 60 seconds.

**OID:** pcrfMIBNotificationsPCMMNoPCEFNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact *My Oracle Support (MOS)*.

## 71805 - PCMM NOCONNECTION PCEF

**Alarm Type:** PCRF

**Description:** PCMM Non Connection to PCEF.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 60 seconds.

**OID:** pcrfMIBNotificationsPCMMNonConnectionPCEFNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact *My Oracle Support (MOS)*.

## 72198 - SMSR SMSC SWITCHED TO PRIMARY

**Alarm Type:** SMS

**Description:** Switched to primary SMSC -- Switched from Secondary to Primary SMSC.

**Default Severity:** Minor

**Instance:** SMSC address

**HA Score:** Normal

**Clearing Action:** Auto clear after 60 minutes

**OID:** SMSRSMSCSwitchedToPrimary

**Recovery:**

No action necessary.

## 72199 - SMSR SMSC SWITCHED TO SECONDARY

**Alarm Type:** SMPP

**Description:** Switched to Secondary SMSC -- Switched from Primary to Secondary SMSC.

**Default Severity:** Minor

**Instance:** SMSC Address

**HA Score:** Normal

**Clearing Action:** Auto clear after 60 minutes

**OID:** 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:** pcrfMIBNotificationsPCMMReachedMaxGatesEventIdNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. 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 -- PCMM reached maximum GPI. A subscriber at IP address ip-addr has reached the configured maximum grants per interval on all upstream gates.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears automatically after 60 seconds.

**OID:** pcrfMIBNotificationsPCMMReachedMaxGPIEventIdNotify

**Recovery:**

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

## 72501 - SCE CONNECTION LOST

**Alarm Type:** PCRF

**Description:** SCE Connection is lost.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Connection to SCE is restored.

**OID:** pcrfMIBNotificationsSCEConnectionLostNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 72549 - SMSR QUEUE FULL

**Alarm Type:** PCRF

**Description:** SMSR queue full -- SMSR internal queue has reached capacity. This will result in messages being dropped until the queue is free to accept new messages.

**Default Severity:** Minor

**Instance:** SMSR queue

**HA Score:** Normal

**Clearing Action:** Auto clear after 60 minutes

**OID:** SMSRQueueFull

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 72559 - SMSR SMSC CONN CLOSED

**Alarm Type:** PCRF

**Description:** SMSC connection closed.

**Default Severity:** Minor

**Instance:** SMSC address

**HA Score:** Normal

**Clearing Action:** Auto clear after 60 minutes or SMSC connection is restored.

**OID:** SMSRSMSCConnectionClosed

**Recovery:**

No action necessary.

## 72565 - SMSR SMTP CONN CLOSED

**Alarm Type:** PCRF

**Description:** SMTP connection closed -- SMTP connection has been closed to MTA {IP Address}.

**Default Severity:** Minor

**Instance:** {hostname of MTA}

**HA Score:** Normal

**Clearing Action:** Auto clear after 60 minutes or SMTP connection is restored.

**OID:** pcrfMIBNotificationsSMSRSMTPConnectionClosedNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 72703 - RADIUS SERVER START FAILED

**Alarm Type:** PCRF

**Description:** RADIUS server start failed.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** N/A

**Clearing Action:** TBD

**OID:** pcrfMIBNotificationsRADIUSServerFailedNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 72706 - RADIUS SERVER CORRUPT AUTH

**Alarm Type:** PCRF

**Description:** RADIUS authenticator is corrupted.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** N/A

**Clearing Action:** TBD

**OID:** pcrfMIBNotificationsRADIUServerCorrupAuthNotify

**Recovery:**

Check the connectivity and cofiguration of the Radius server.

## 72904 - DIAMETER TOO BUSY

**Alarm Type:** PCRF

**Description:** Diameter load shedding set a busy state.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** The Diameter load drops below admission criteria thresholds or this alarm clears automatically after 30 seconds.

**OID:** pcrfMIBNotificationsDiameterTooBusyNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact *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:** pcrfMIBNotificationsRadiusTooBusyNotify

**Recovery:**

If this alarm occurs infrequently, then monitor the health of the system. If this alarm occurs frequently, contact *My Oracle Support (MOS)*.

## 74000 - POLICY CRITICAL ALARM

**Alarm Type:** PCRF

**Description:** Critical Policy alarm.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm can be cleared by a policy or clears automatically after 3600 seconds (one hour).

**OID:** pcrfMIBNotificationsPolicyServerCriticalAlarmNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 74001 - POLICY MAJOR ALARM

**Alarm Type:** PCRF

**Description:** Major Policy alarm.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm can be cleared by a policy or clears automatically after 3600 seconds (one hour).

**OID:** pcrfMIBNotificationsPolicyServerMajorAlarmNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 74002 - POLICY MINOR ALARM

**Alarm Type:** PCRF

**Description:** Minor Policy alarm.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm can be cleared by a policy or clears automatically after 3600 seconds (one hour).

**OID:** pcrfMIBNotificationsPolicyServerMajorAlarmNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 74020 - DELETE EXPIRE FILES

**Alarm Type:** PCRF

**Description:** Delete expire files -- Stats Files Generator Task has removed some files which weren't synced to remote servers (<external system IP>,<external system IP>, etc).

**Default Severity:** Major

**Instance:** Stats files generator

**HA Score:** Normal

**Clearing Action:** Auto clear 300 seconds

**OID:** StatsFilesGeneratorDeleteExpireFiles

**Recovery:**

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

## 74021 - FILE SYNCHRONIZATION FAILURE

**Alarm Type:** PCRF

**Description:** Files synchronization failure -- Stats Files Synchronization #<X> task failed to sync local to remote server (<external system Host Name/IP>) after retry <N> times, where:

- X: task #
- N: 1-5 retry times
- External system Host Name/IP: user-defined remote server's address to which files are synced

**Default Severity:** Minor

**Instance:** Stats files synchronization

**HA Score:** Normal

**Clearing Action:** Auto clear 300 seconds

**OID:** pcrfMIBNotificationsFilesSynchronizationFailureNotify

**Recovery:**

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

## 74022 - FILES UPLOADING FAILURE

**Alarm Type:** PCRF

**Description:** PM Statistics Files Uploading Task failed to upload local stat files to FTP server *FTP server Host Name/IP* after retry *number* times.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Auto clear 300 seconds

**OID:** FilesUploadingFailureNotify

**Recovery:**

1. Fix network problems or verify FTP configuration info, which is defined in the scheduler task of CMP.
2. If 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 clear when task runs again.

**OID:** pcrfMIBNotificationsCmtsSubnetOverlappedNotify

**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, do the previous steps again.

## 74602 - QP Multiple Active In Cluster Failure

**Alarm Type:** QP

**Description:** Multiple Active servers have been detected in the same cluster; the cluster is in Split Brain state.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears when HA recovers or can clears automatically after 30 minutes. When HA recovers there will be only one Active server in a cluster.

**OID:** pcrfMIBNotificationsQPMultipleActiveInClusterFailureNotify

**Recovery:**

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

## 74603 - QP Max Primary Cluster Failure Threshold

**Alarm Type:** QP

**Description:** The number of failed MPE pairs reaches the threshold of *the configured threshold value* at *the site name.*

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears when the number of failed MPE pairs remain at a lower value than the threshold of {Max Primary Site Failure Threshold} at {Site}, or clears automatically after 30 minutes.

**OID:** pcrfMIBNotificationsQPMaxMPEPrimaryClusterFailureNotify

**Recovery:**

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

## 74604 - QP Policy Cluster Offline Failure

**Alarm Type:** QP

**Description:** Policy Cluster is offline.

**Default Severity:** Critical

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** This alarm clears when a server in the MPE cluster comes online. The alarm clears automatically after 30 minutes.

**OID:** pcrfMIBNotificationsQPMPEClusterOfflineFailureNotify

**Recovery:**

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

**Recovery:**

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

## 75000 - POLICY LIBRARY LOADING FAILED

**Alarm Type:** PCRF

**Description:** Policy library loading failed -- PCRF was unable to load the latest policy library. If this alarm occurred at startup time or at failover, this indicates the PCRF does not have any policies deployed. If this alarm occurred on a new policy push when PCRF was running with some existing policies, this alarm indicates that the PCRF will continue to run with those existing policies.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Performing a reapply config may fix the problem.

**OID:** pcrfMIBNotificationsPolicyLoadingLibraryFailedNotify

**Recovery:**

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

### 75105 - Mediation SOAP load shedding set a busy state

**Alarm Type:** Mediation

**Description:** The Mediation Server SOAP provisioning interface has become busy, and has begun load shedding.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** MediationSOAPTooBusyNotify

**Recovery:**

No action required.

### 75106 - SPR: Create connection to SPR *ip-address* failed

**Alarm Type:** Mediation

**Description:** Create connection to SPR *ip-address* failed.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** SPRConnectionFailedNotify

**Recovery:**

No action required.

### 75107 - Sync: Backup folder disk quota exceeded. Disk quota: *percentage*, total usage: *space used*

**Alarm Type:** Mediation

**Description:** Mediation sync directory disk quota has been exceeded.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** MSDiskQuotaExceedNotify

**Recovery:**

No action required.

### 75108 - No space left on device

**Alarm Type:** Mediation

**Description:** No space left on device.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** MSDiskNoSpaceNotify

**Recovery:**

No action required.

### 75109 - The Mediation Server has achieved 80% of the maximum number of users in SPR.

**Alarm Type:** Mediation

**Description:** Achieve 80% maximum number of users in SPR.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** SPRLicenselimitNotify

**Recovery:**

No action required.

### 77904 - BOD PCMM TOO BUSY

**Alarm Type:** PCRF

**Description:** BOD PCMM TOO BUSY

**Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Clears automatically after 30 seconds.

**OID:** pcrfMIBNotificationsBODPCMMTooBusyNotify

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 77905 - BOD DIAMETER TOO BUSY

**Alarm Type:** PCRF

**Description:** BOD DIAMETER TOO BUSY

**Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Clears automatically after 30 seconds.

**OID:** pcrfMIBNotificationsBODDiameterTooBusyNotify

**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 in one hour by auto clear.

**OID:** pcrfMIBNotificationsADSConnectionLostNotify

**Recovery:**

1. Check configuration and availability of the analytics client.
2. Check the client for reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (port 222) is operational.
4. If the problem persists, contact *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 when a policy change is made or a Reapply Configuration is performed. It can be raised by the standby during startup if it was unable to get the policy jar file from the active during startup.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** Since the alarm can be raised by both the active and standby servers, the alarm will not clear once the problem is fixed; it will auto-clear in an hour.

**OID:** pcrfMIBNotificationsRsyncFailedNotify

**Recovery:**

1. This alarm can be ignored during a mixed version upgrade (eg. 7.5/7.6 -> 9.1) and when rebooting both servers on the MPE.
2. If the alarm is seen on the MRA, it indicates the logback config files are not transferring, which is harmless to the operation.
3. The most likely cause is that the ssh keys have not been exchanged; ensure they are exchanged correctly.
4. Perform a Reapply Configuration.
5. If performing a Reapply Configuration does not fix the problem, another alarm will be raised by the active server for that particular operation. If the problem persists, contact *My Oracle Support (MOS)*.
6. The original alarm will auto-clear in an hour.

## 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:** pcrfMIBNotificationsSessDBSizeReachedThresholdNotify

**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 - AVERAGE_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:** Clears automatically after 3600 seconds.

**OID:** pcrfMIBNotificationsAvgSessSizeReachedThresholdNotify

**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 3600 seconds.

**OID:** pcrfMIBNotificationsBindDBSizeReachedThresholdNotify

**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 - AVERAGE_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:** Clears automatically after 3600 seconds.

**OID:** pcrfMIBNotificationsAvgBindSizeReachedThresholdNotify

**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 interface load shedding set a busy state

**Alarm Type:** Mediation

**Description:** Mediation SOAP interface load shedding set a busy state, some requests will be rejected.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** MediationSOAPTooBusy

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79106 - Create connection to SPR

**Alarm Type:** Mediation

**Description:** Mediation created connection to SPR failed.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** SPRConnectionFailed

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79107 - Sync: Backup folder disk quota exceeded

**Alarm Type:** Mediation

**Description:** Mediation server backup folder of sync function exceeds quota.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A.

**OID:** MediationDiskQuotaExceed

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79108 - Sync: Backup folder disk quota exceeded.

**Alarm Type:** Mediation

**Description:** No space left on Mediation server.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** MediatonDiskNoSpace

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79109 - 80% maximum number of users in SPR achieved.

**Alarm Type:** Mediation

**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 - PM Stats File Upload Fail, PM Stats File Upload Fail Clear

**Alarm Type:** PCRF

**Description:**

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** NA

**OID:** StatsFileUploadFailure

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79120 - Batch Folder Disk Quota Exceeded

**Alarm Type:** Mediation

**The batch folder disk quota has been exceeded.**

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** BatchDiskQuotaExceeds

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79995 - X1 Connection Lost, Clear X1 Alarm

**Alarm Type:** PCRF

**Description:** The X1 connection has been lost.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** X1ConnectionLost

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

### 79996 - X2 Connection Lost, Clear X2 Alarm

**Alarm Type:** PCRF

**Description:** The X2 connection has been lost.

**Default Severity:** Minor

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** X2ConnectionLost

**Recovery:**

If the problem persists, contact *My Oracle Support (MOS)*.

## 80001 - QP DB State Transition

**Alarm Type:** QP

**Description:** The DB status of the blade is not fully ready -- The MySQL database manager generates a "MySQL state transition" event every time it makes a state-machine transition. The event text describes the transition.

**Default Severity:** Info

**Instance:** MySQL

**HA Score:** Normal

**Clearing Action:** This alarm is cleared by qp-procmgr as qp-procmgr shuts down.

**OID:** pcrfMIBNotificationsQPDBStateChangeNotify

**Recovery:**

No action required.

## 80002 - QP MySQL Relay Log Dropped

**Alarm Type:** QP

**Description:** A portion of the MySQL relay log was dropped as the slave was shutting down -- This event is raised when a slave server times out while trying to apply its relay log during a slave stop. The server may not be hurt, but there may be aftereffects. This event is raised to trigger a debug for possible aftereffects.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPMySQLRelayLogDroppedNotify

**Recovery:**

Debug the system for possible aftereffects caused by the timeout.

## 80003 - QP MySQL Database Level Advertisement

**Alarm Type:** QP

**Description:** The ranking of slaves when the master is outdated -- If the master database is outdated, the server raises this event once per minute. The server will rank the slaves, from best to worst, based on their database level .

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsQPMySQLDBLevelNotify

**Recovery:**

Use the information of this event to help resolve an outdated master database raised by alarm 70020.

## 82704 - BINDING RELEASE TASK

**Alarm Type:** PCRF

**Description:** Binding Release Task -- The binding release task has started, completed, or aborted.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsBindingReleaseTaskNotify

**Recovery:**

No action required.

## 84004 - POLICY INFO EVENT

**Alarm Type:** PCRF

**Description:** Policy Info Event -- Application is ready.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsPolicyInfoEventNotify

**Recovery:**

No action required.

## 86001 - APPLICATION IS READY

**Alarm Type:** PCRF

**Description:** Application is ready for service.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsApplicationIsReadyNotify

**Recovery:**

No action required.

### 86100 - CMP USER LOGIN

**Alarm Type:** PCRF

**Description:** CMP User login was succesful.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsCMPUserLoginNotify

**Recovery:**

No action required.

### 86101 - CMP USER LOGIN FAILED

**Alarm Type:** PCRF

**Description:** CMP User login failed.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsCMPUserLoginFailedNotify

**Recovery:**

No action required.

### 86102 - CMP USER LOGOUT

**Alarm Type:** PCRF

**Description:** CMP User performed logout.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsCMPUserLogoutNotify

**Recovery:**

No action required.

## 86200 - CMP USER PROMOTED SERVER

**Alarm Type:** PCRF

**Description:** CMP User promoted server -- Application is ready.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsCMPUserPromotedServerNotify

**Recovery:**

No action required.

## 86201 - CMP USER DEMOTED SERVER

**Alarm Type:** PCRF

**Description:** CMP User demoted either CMP 1 or CMP 2.

**Default Severity:** Info

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:**pcrfMIBNotificationsCMPUserDemotedServerNotify

**Recovery:**

No action required.

## 86300 - SH ENABLE FAILED

**Alarm Type:** PCRF

**Description:** Enable Sh Connection failed -- The CMP performed a global operation to enable Sh on all MPE's and it failed on the specified MPE.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsCMPShConEnableFailedNotify

**Recovery:**

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

## 86301 - SH DISABLE FAILED

**Alarm Type:** PCRF

**Description:** Disable Sh Connection failed -- The CMP performed a global operation to disable Sh on all MPE's and it failed on the specified MPE.

**Default Severity:** Major

**Instance:** N/A

**HA Score:** Normal

**Clearing Action:** N/A

**OID:** pcrfMIBNotificationsCMPShConDisableFailedNotify

**Recovery:**

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

## 86303 - NMP Apply failed Clear, NMP Apply failed Set

**Alarm Type:** PCRF

**Description:** If NW-CMP fails to apply the configuration changes to any S-CMP, then the alarm will be raised on the NW-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 - SCMP Unreachable Clear, SCMP Unreachable Set

**Alarm Type:** PCRF

**Description:** If an 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 - SCMP Split brain Clear, SCMP Split brain Set

**Alarm Type:** PCRF

**Description:** When a geo-redundant S-CMP is in split brain (both site is reporting to be Primary), here will be an alarm 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 - SMP Apply Failed Clear, SMP Apply Failed Set

**Alarm Type:** PCRF

**Description:** When a (S)CMP failed to apply settings to any MRA or MPE, here will be a newly defined alarm 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/MPE is successful.

## 86307 - SMP Sync Failed Clear, SMP Sync Failed Set

**Alarm Type:** PCRF

**Description:** If the connection between the NW-CMP and the S-CMP is broken and any of the above 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 sync is successful in the next cycle.

## 86308 - NCMP Ref ObjClear, NCMP Ref Obj Set

**Alarm Type:** PCRF

**Description:** When a top level object is referred by S-CMP but has been deleted in NW-CMP, this alarm will be raised in NW-CMP.

**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.

# Glossary

**A**

| | |
|---|---|
| AM | application manager<br>A server within a network that is responsible for establishing and managing subscriber sessions associated with a specific application. |

**B**

| | |
|---|---|
| B-RAS | broadband remote access server |

**C**

| | |
|---|---|
| CMP | Configuration Management Platform<br>A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface. |
| CMTS | Cable modem termination system<br>An edge device connecting to subscribers' cable modems in a broadband network. A CMTS device can function as a PCEF device; see PCEF.<br>Cable Modem Termination System: Equipment used by cable companies to provide high speed data services to cable subscribers. |

**D**

| | |
|---|---|
| DNS | Domain Name System |

**D**

| | |
|---|---|
| | A system for converting Internet host and domain names into IP addresses. |
| DQoS | Dynamic Quality of Service<br>A COPS-based protocol that is part of the Packet Cable standards used to communicate between a CMS and a CMTS for setting up voice calls. An MPE device can be inserted between these two entities to apply additional policy rules as sessions are established. |

**G**

| | |
|---|---|
| GUI | Graphical User Interface<br>The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands. |

**H**

| | |
|---|---|
| HA | High Availability<br>High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages. |
| HP | Hewlett-Packard |

**M**

| | |
|---|---|
| MPE | Multimedia Policy Engine<br>A high-performance, high-availability platform for operators to deliver and manage differentiated services over high-speed data networks. The MPE includes a |

**M**

| | |
|---|---|
| | 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<br>Scales the Policy Management infrastructure by distributing the PCRF load across multiple Policy Server devices. |
| MTA | Major Trading Area |
| Multimedia Policy Engine | See MPE. |
| Multiprotocol Routing Agent | See MRA. |

**N**

| | |
|---|---|
| NTP | Network Time Protocol |
| NTP daemon | Network Time Protocol daemon – NTP process that runs in the background. |

**O**

| | |
|---|---|
| OID | Object Identifier<br>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 |

**O**

| | |
|---|---|
| | managed objects for their own products. |

**P**

| | |
|---|---|
| PCRF | Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network.<br>Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF. |

**Q**

| | |
|---|---|
| QBus Platform | See QP. |
| QP | QBus Platform<br>Software that provides an execution environment for Java-based applications, providing common interfaces into databases, event logging, SNMP, and cluster state. |

**R**

| | |
|---|---|
| REPL | Replication |

**S**

| | |
|---|---|
| SMSR | SMS Relay Application<br>An interface between the MPE and SMSC or other specific SMS web service(s). |
| SNMP | Simple Network Management Protocol. |

**S**

| | |
|---|---|
| | An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups. |
| SOAP | Simple Object Access Protocol |
| SPC | Service Provisioning over COPS (Common Open Policy Service protocol) |