Oracle® Communications Diameter Signaling Router

Alarms and KPIs Reference

E57505 Revision 01

February 2015

ORACLE®

Oracle® Communications Alarms and KPIs Reference

Table of Contents

Chapter 5: Key Performance Indicators (KPIs)....................................356

Glossary...368

List of Figures

List of Tables

Chapter

1

Introduction

Topics:

This section contains an overview of the available information for DSR alarms and events. The contents include sections on the scope and audience of the documentation, as well as how to receive customer support assistance.

Overview

The *DSR Alarms and KPIs* documentation provides information about DSR alarms, events, and KPIs provides corrective maintenance procedures, and other information used in maintaining the system.

- Information relevant to understanding alarms and events that may occur on the application
- Recovery procedures for addressing alarms and events, as necessary
- Procedures for viewing alarms and events, generating alarms reports, and viewing and exporting alarms and event history
- Information relevant to understanding KPIs in the application
- The procedure for viewing KPIs
- Lists of KPIs

Scope and Audience

This manual does not describe how to install or replace software or hardware.

This manual is intended for personnel who must maintain operation of the DSR. The manual provides lists of alarms, events, and KPIs along with preventive and corrective procedures that will aid personnel in maintaining the DSR.

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

Manual Organization

Information in this document is organized into the following sections:

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

Documentation Admonishments

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

Table 1: Admonishments

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

Related 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

User Interface Introduction

Topics:

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

User Interface Organization

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

DSR GUI

In a DSR, the following Main Menu options are accessible from the System OAM (SOAM) server:

- Transport Manager
- Communication Agent
- SS7/Sigtran
- Diameter Common
- Diameter
- RBAR
- FABR
- Policy and Charging
- IPFE
- MAP-Diameter IWF
- CPA

The following Main Menu options are accessible from the Network OAM (NOAM) server:

- Communication Agent
- Diameter Common > Network Identifiers > MCCMNC, MCCMNC Mapping
- Diameter > Configuration for Topology Hiding,
- Network-wide Policy and Charging > Configuration components are configurable on the NOAM; some Configuration components are view-only on the SOAM. Policy and Charging > Maintenance components are accessible on the NOAM only.
- MAP-Diameter IWF

Bulk Import and Bulk Export functions appear on both OAMs, to be used for the data that can be configured on that OAM.

Most other Main Menu options are configurable from the Network OAM server and view-only from the System OAM server.

User Interface Elements

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

Table 2: User interface elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.

Element	Location	Function
Session Banner	Next bar across the top of the web page	The left side of the banner just above the Main Menu provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner: • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates that a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • **Page Title Area**: Occupies the top of the work area. It displays the title of the current page being displayed, the date and time, and includes a link to context-sensitive help. • **Page Control Area**: Is located below the Page Title Area, and is used to show controls for the Page Area (this area is optional). When available for an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • **Page Area**: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is

Element	Location	Function
		provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Splash Page Welcome Message*.

Main Menu Options

Table 3: Main Menu Options describes all main menu user interface options.

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

Note: Some menu items are configurable only on the NOAM and view-only on the SOAM; and some menu options are configurable only on the SOAM. See *DSR GUI*.

Note: Some features will not appear in the main menu until the features are activated.

Table 3: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Manage licenses and upgrades • Authenticate LDAP servers • Configure SNMP trapping services • Validate and transfer ISO files • Prepare, initiate, monitor, and complete upgrades • View the software versions report • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes

Menu Item	Function
	• Services • Servers • Server Groups • Resource Domains • Places • Place Associations On the SOAM, allows the user to configure the NOAM list plus Interface and Port DSCP.
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status & Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, and data file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager	Allows the user to configure adjacent nodes, configuration sets, or transports; and edit transports.
Communication Agent	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	Allows the user to configure various users, groups, remote signaling points, links and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data.
Diameter Common	Allows the user to configure: • Network Identifiers: on the NOAM - MCC Ranges • Network Identifiers on the SOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile assignments The DSR Bulk Import and Export functions are available on both OAMs for the data that is configured on that OAM.
Diameter	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAM, Diameter Topology Hiding configuration

Menu Item	Function
	• On the SOAM, Diameter Configuration, AVP Dictionary and Troubleshooting for IDIH configuration; Diameter Mediation configuration: and Maintenance functions
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only.

Policy and Charging
(optional)
	On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	
	• General Options
	• Access Point Names
	• Policy DRA
	
	    • PCRF Pools
	    • PCRF Sub-Pool Selection Rules
	    • Network-Wide Options
	
	• Online Charging DRA
	
	    • OCS Session State
	    • Realms
	    • Network-Wide Options
	
	• Alarm Settings
	• Congestion Options
	
	On the NOAM, allows the user to perform maintenance tasks, edit options, and view elements for:
	
	• Maintenance
	
	    • SBR Status

Menu Item	Function

	• Policy Database Query
	
	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	
	• General Options
	• Access Point Names
	• Policy DRA
	
	    • PCRFs
	    • Binding Key Priority
	    • PCRF Pools
	    • PCRF Pool to PRT Mapping
	    • PCRF Sub-Pool Selections
	    • Policy Clients
	    • Site Options
	
	• Online Charging DRA
	
	    • OCSs
	    • CTFs
	    • OCS Session State
	    • Realms
	
	• Error Codes
	• Alarm Settings
	• Congestion Options

Gateway Location Application (Optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP).
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only.
MAP-Diameter Interworking	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAM, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application: • MD-IWF Options • Diameter Realm

Menu Item	Function
	• Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping
CPA (Charging Proxy Application) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • System Options • Message Copy • Session Binding Repository • SBR Subresource Mapping This is accessible from the SOAM only.
Help	Launches the Help system for the user interface.
Logout	Allows the user to log out of the user interface.

Missing Main Menu options

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

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

Common Graphical User Interface Widgets

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

Supported Browsers

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

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing a password upon login. The System Login page also features a current date and time stamp and a customizable login message.

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

Customizing the Login Message

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

ORACLE

WELCOME

Welcome to the Configuration Management Platform (CMP). Please enter your user name and password below to access the CMP desktop. If you do not have an existing user name or password, or if you have misplaced either, please contact the system administrator.

USERNAME [   ]

PASSWORD [   ]
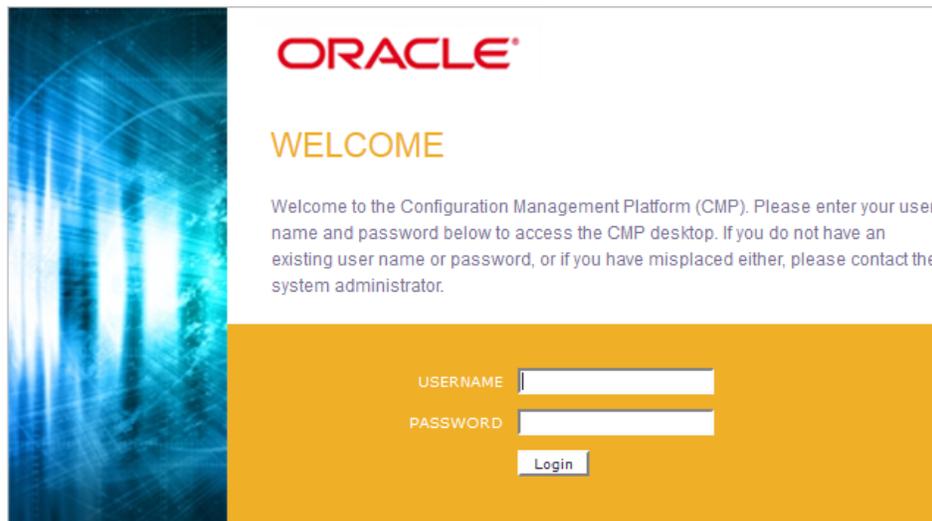
[Login]

Figure 1: Oracle System Login

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

   The **General Options Administration** page appears.

2. Locate **LoginMessage** in the **Variable** column.

3. Enter the login message text in the **Value** column.

4. Click **OK** or **Apply** to submit the information.

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

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

Accessing the DSR Graphical User Interface

In a DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you will access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM** > **Administration** > **Access Control > Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example https://dsr-no.yourcompany.com.

    When using Single Sign-On, you cannot use the IP address of the server.

2. When prompted by the browser, confirm that the server can be trusted.
    The System Login page appears.

3. Enter the Username and Password for your account.
    The DSR GUI for the NOAM appears.

4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.
    The DSR GUI for the SOAM appears.

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

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

Table 4: Main Menu icons
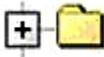
Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) will collapse the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.

Icon	Name	Description
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, you will see a variety of page formats. Tables, forms, tabbed pages, and reports are the most common formats in the user interface.

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

Tables

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

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

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

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

Figure 2: Paginated table

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

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

Export

Figure 3: Scrollable table

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

Forms

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

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

Ok   Apply   Cancel

Figure 4: Form page

Tabbed pages

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

Figure 5: Tabbed pages

Figure 6: Tabbed pages

Reports

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

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

User Account Usage Report

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

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


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

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


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

End of User Account Usage Report

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

Figure 7: Report output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the **User Interface** splash page appears. You can display a customized welcome message on the **User Interface** splash page. Use this procedure to customize the message.

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

   The **General Options Administration** page appears.

2. Locate **WelcomeMessage** in the **Variable** column.

3. Enter the welcome message text in the **Value** column.

4. Click **Update OK** or **Apply** to submit the information.

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

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

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See *Figure 8: Sorting a Table by Column Header*. Clicking the column header again reverses the direction of the sort.

Local Node Name ▼	Realm	FQDN	SCTP Listen Port	TCP Listen Port	Connection Configuration Set	CEX Configuration Set	IP Addresses

Figure 8: Sorting a Table by Column Header

Page Controls

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

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

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

Table 5: Example Action buttons

Action button	Function
Insert	Insert data into a table
Edit	Edit data within a table
Delete	Delete data from table
Change	Change the status of a managed object

Some Action buttons take you to another page.

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

Table 6: Submit buttons

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

Clear Field Control

The clear field control is a widget that allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

Click the **X** next to a pulldown list to clear the field.
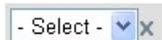
Figure 9: Clear Field Control X

Optional Layout Element Toolbar

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

Figure 10: Optional Layout Element Toolbar

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

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

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.
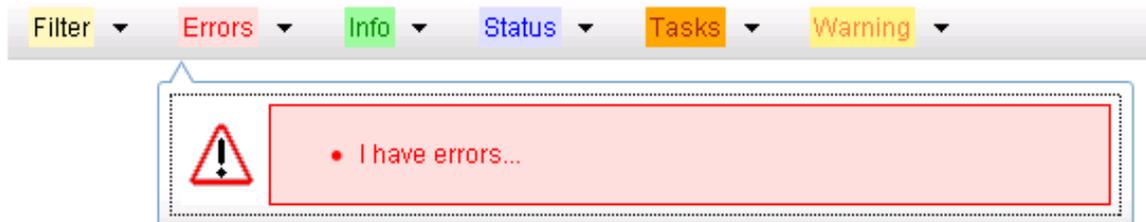
Figure 11: Automatic Error Notification

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

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

Opening an Element in the Toolbar

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

1. Click the text of the element or the triangle icon to open an element.
   The selected element opens and overlays the work area.
2. Click **X** to close the element display.

Filters

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

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

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

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

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

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

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.
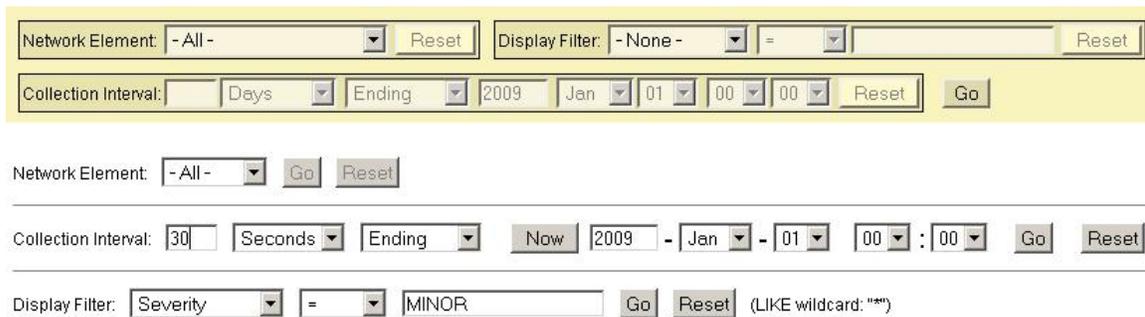
Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter control elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.

Operator	Description
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

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

Filtering on the Network Element

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

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

Records are displayed according to the specified criteria.

Filtering on Collection Interval

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

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

   The duration must be a numeric value.

3. Select a unit of time from the pulldown menu.

   The unit of time can be seconds, minutes, hours, or days.

4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering using the Display Filter

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

1. Click **Filter** in the optional layout element toolbar.

The filter tool appears.

2. Select a field name from the **Display Filter** pulldown menu.

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

   The selected field name displays in the **Display Filter** field.

3. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.

4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (**=**) operator and a value of MINOR, the table would show only records where Severity=MINOR.

5. For data tables that support compound filtering, click the **Add** button to add another filter condition. Then repeat steps 2 through 4.
   Multiple filter conditions are joined by an AND operator.

6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Pause Updates

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

Max Records Per Page Controls

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

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

   The **General Options Administration** page appears.

2. Change the value of the **MaxRecordsPerPage** variable.

   Note: MaxRecordsPerPage has a range of values from 10 to 100 records. The default value is 20.

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

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Alarms, Events, and KPIs Overview

Topics:

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

Help Organization

Information in this document is organized into the following sections:

- *Alarms, Events, and KPIs Overview* provides general information about the application's alarms, events, and KPIs.
- *Alarms and Events* provides information and recovery procedures for alarms and events, organized first by alarm category, then numerically by the number that appears in the application.
- *Key Performance Indicators (KPIs)* provides detailed KPI information, organized alphabetically by KPI name.

Alarms Warning

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

General alarms and events information

This section provides general information about alarms and events, including an alarms overview, types of alarms/events, and alarms-related procedures.

Alarms and events overview

Alarms provide information pertaining to a system's operational condition that a network manager may need to act upon. An alarm might represent a change in an external condition, for example, a communications link has changed from connected to disconnected state. Alarms can have these severities:

- Critical application error
- Major application error
- Minor application error
- Cleared

An alarm is considered inactive once it has been cleared and cleared alarms are logged on the **Alarms & Events** > **View History** page of the GUI.

Events note the occurrence of a transient condition. Events have a severity of Info and are logged on the **View History** page.

Note: Some events may be throttled because the frequently generated events can overload the MP or OAM server's system or event history log (e.g., generating an event for every ingress message failure). By specifying a throttle interval (in seconds), the events will appear no more frequently than once during the interval duration period (e.g., if the throttle interval is 5-seconds, the event will be logged no frequently than once every 5-seconds).

The following figure shows how Alarms and Events are organized in the application.
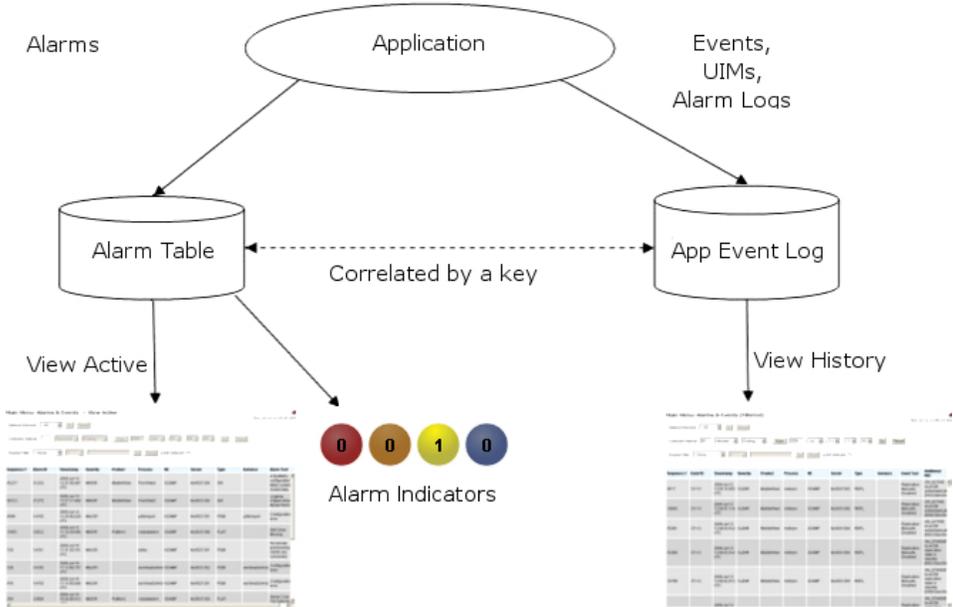
Figure 13: Flow of Alarms

Alarms and events are recorded in a database log table. Application event logging provides an efficient way to record event instance information in a manageable form, and is used to:

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

Alarm indicators, located in the User Interface banner, indicate all critical, major, and minor active alarms. A number and an alarm indicator combined represent the number of active alarms at a specific level of severity. For example, if you see the number six in the orange-colored alarm indicator, that means there are six major active alarms.

Figure 14: Alarm Indicators Legend

Figure 15: Trap Count Indicator Legend

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of alarm types see *Alarm and event types*.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm
- Instance: the instance of a managed object for which an alarm or event is generated.

  Note: The value in the Instance field can vary, depending on the process generating the alarm.

- HA Score: high availability score; determines if switchover is necessary
- Auto Clear Seconds: the number of seconds that have to pass before the alarm will clear itself.

  Note: Some alarms and events have an Auto Clear Seconds of 0 (zero), indicating that these alarms and events do not auto-clear

- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

Alarm and event ID ranges

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

Table 8: Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5099
OAM	10000-10999
IDIH	11500-11549
SBR	12000-12999
ComAgent	19800-19909
DSR Diagnostics	19910-19999
Diameter	22000-22350, 22900-22999
RBAR	22400-22424
Generic Application	22500-22599

Application/Process Name	Alarm ID Range
FABR	22600-22640
PDRA	22700-22799
CPA	22800-22849
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32700
DM-IWF	33000-33024
Load Generator	33025-33049
MD-IWF	33050-33099
GLA	33100-33149

Alarm and event types

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

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

Table 9: Alarm and Event Types

Type Name	Type
APPL	Application
CAF	Communication Agent (ComAgent)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
CHG	Charging
CNG	Congestion Control
COLL	Collection
CPA	Charging Proxy Application
DB	Database
DIAM	Diameter
DISK	Disk
DNS	Domain Name Service
DPS	Data Processor Server

Type Name	Type
ERA	Event Responder Application
FABR	Full Address Based Resolution
HA	High Availability
HSS	Home Subscriber Server
IDIH	Integrated DIH
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOADGEN	Load Generator
LOG	Logging
MEAS	Measurements
MEM	Memory
NP	Number Portability
OAM	Operations, Administration & Maintenance
PDRA	Policy DRA
pSBR	Policy SBR
PLAT	Platform
PROC	Process
PROV	Provisioning
NAT	Network Address Translation
RBAR	Range-Based Address Resolution
REPL	Replication
SBRA	Session Binding Repository Application
SCTP	Stream Control Transmission Protocol
SDS	Subscriber Database Server
SIGC	Signaling Compression
SIP	Session Initiation Protocol Interface
SL	Selective Logging
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack

Type Name	Type
SW	Software (generic event type)
TCP	Transmission Control Protocol

Viewing active alarms

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

Use this procedure to view active alarms.

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

1. Select **Alarms & Events > View Active**.
    The **View Active** page appears.

2. If necessary, specify filter criteria and click **Go**.
    The active alarms are displayed according to the specified criteria.

    The active alarms table updates automatically. When new alarms are generated, the table is automatically updated, and the view returns to the top row of the table.

3. To suspend automatic updates, click any row in the table.
    The following message appears: `(Alarm updates are suspended.)`

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

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

Active alarms data export elements

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

Table 10: Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-).

Element	Description	Data Input Notes
		Description must begin with an alphanumeric character.
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting active alarms

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

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Alarm details can be exported to a file by clicking the **Export** button on the **View Active** page. The system automatically creates and writes the exported active alarm details to a CSV file in the file management area.

If filtering has been applied in the **View Active** page, only filtered, active alarms are exported.

Use this procedure to export active alarms to a file.Use this procedure to schedule a data export task.

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

The **Schedule Active Alarm Data Export** page appears.

4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Active alarms data export elements* .

5. Select the **Export Frequency**.

6. Select the **Time of Day**.

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

7. Select the **Day of Week**.

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

8. Click **OK** or **Apply** to initiate the active alarms export task.

   From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see *Displaying the file list*.

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

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

9. Click **Export**.
   The file is exported.

10. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

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

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

Generating a report of active alarms

Use this procedure to generate a report.

1. Select **Alarms & Events > View Active**.

   The **View Active** page appears.

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

3. Click **Report**.
   The View Active Report is generated. This report can be printed or saved to a file.

4. Click **Print** to print the report.

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

Viewing alarm and event history

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

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

1. Select **Alarms & Events > View History** .
   The **View History** page appears.

2. If necessary, specify filter criteria and click **Go**.

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

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

   The historical alarms table updates automatically. When new historial data is available, the table is automatically updated, and the view returns to the top row of the table.

3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

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

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

Historical events data export elements

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

Table 11: Schedule Event Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.

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

Exporting alarm and event history

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

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

The details of historical alarms and events can be exported to a file by clicking the **Export** button on the **View History** page. The system automatically creates and writes the exported historical alarm details to a CSV file in the file management area.

If filtering has been applied in the **View History** page, only filtered historical alarms and events are exported. Use this procedure to export alarm and event history to a file. Use this procedure to schedule a data export task.

1. Select **Alarms & Events > View History**.
   The **View History** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Event Data Export** page appears.
4. Enter the **Task Name**.

For more information about **Task Name**, or any field on this page, see *Historical events data export elements* .

5. Select the **Export Frequency**.

6. If you selected Hourly, specify the **Minutes.**

7. Select the **Time of Day**.

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

8. Select the **Day of Week**.

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

9. Click **OK** or **Apply** to initiate the data export task.

   The data export task is scheduled. From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see *Displaying the file list*.

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

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

10. Click **Export**.
    The file is exported.

11. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

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

    From the **Status & Manage > Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see .

Generating a report of historical alarms and events

Use this procedure to generate a report.

1. Select **Alarms & Events > View History**.

   The **View History** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.

3. Click **Report**.
   The View History Report is generated. This report can be printed or saved to a file.

4. Click **Print** to print the report.

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

Displaying the file list

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

1. From the Main menu, select **Status & Manage > Files**.

   The **Status & Manage Files** page appears.

2. Select a server.
   All files stored on the selected server are displayed.

Data Export

From the Data Export page you can set an export target to receive exported performance data. Several types of performance data can be filtered and exported using this feature. For more information about how to create data export tasks, see:

- *Exporting active alarms*
- *Exporting alarm and event history*
- *Exporting KPIs*

From the Data Export page you can manage file compression strategy and schedule the frequency with which data files are exported.

Data Export elements

This table describes the elements on the Data Export page.

Table 12: Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server.	Must be a valid hostname, IPv4 address, or IPv6 address. Range: Maximum length is 255 characters; alphanumeric characters (a-z, A-Z, and 0-9) and minus sign. Hostname must start and end with an alphanumeric. To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None

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

Element	Description	Data Input Notes
Time of Day	If the Upload Frequency is Daily of Weekly, this is the time of day the export occurs	Format: Time textbox Range: HH:MM AM/PM in 15-minute increments Default: 12:00 AM
Day of Week	If Upload Frequency is Weekly, this is the day of the week when exported data files will be transferred to the export server	Format: Radio button Range: Sunday through Saturday Default: Sunday
SSH Key Exchange	This button launches a dialog box. The dialog requests username and password and initiates SSH key exchange.	Format: Button
Transfer Now	This button initiates an immediate attempt to transfer any data files in the export directory to the export server.	Format: Button

Configuring data export

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

1. Select **Administration > Remote Servers > Data Export**.
   The Data Export page appears.
2. Enter a **Hostname**.
   See the Data Export elements for details about the **Hostname** field and other fields that appear on this page.
3. Enter a **Username**.
4. Enter a **Directory Path** on the Export server.
5. Enter the **Path to Rsync** on the Export server.
6. Select whether to enable the transfer of the backup file. To leave the backup disabled, do not check the box.
7. Select the **File Compression** type.
8. Select the **Upload Frequency**.
9. If you selected hourly for the upload frequency, select the **Minute** intervals.
10. If you selected daily or weekly for the upload frequency, select the **Time of Day**.
11. If you selected weekly for the upload frequency, select the **Day of the Week**.
12. Click **Exchange SSH Key** to transfer the SSH keys to the export server.
    A password dialog box appears.
13. Enter the password.
    The server will attempt to exchange keys with the specified export server. After the SSH keys are successfully exchanged, continue with the next step.

14. Click **OK** or **Apply**.

The export server is now configured and available to receive performance and configuration data.

Tasks

The **Tasks** pages display the active, long running tasks and scheduled tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results for long running tasks, while the **Scheduled Task**s page provides a location to view, edit, and delete tasks that are scheduled to occur.

Active Tasks

The **Active Tasks** page displays the long running tasks on a selected server. The **Active Tasks** page provides information such as status, start time, progress, and results, all of which can be generated into a report. Additionally, you can pause, restart, or delete tasks from this page.

Active Tasks elements

The **Active Tasks** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes elements on the **Active Tasks** page.

Table 13: Active Tasks Elements

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

Deleting a task

Use this procedure to delete one or more tasks.

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

The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select one or more tasks.

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

   Note: You can select multiple rows to delete at one time. To select multiple rows, press and hold Ctrl as you click to select specific rows.

4. Click **Delete**.
   A confirmation box appears.

5. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Deleting all completed tasks

Use this procedure to delete all completed tasks.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Click **Delete all Completed**.
   A confirmation box appears.

4. Click **OK** to delete all completed tasks.
   All tasks with the status of completed are deleted.

Canceling a running or paused task

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

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select a task.

4. Click **Cancel**.
   A confirmation box appears.

5. Click **OK** to cancel the selected task.

The selected task is canceled.

Pausing a task

Use this procedure to pause a task.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select a task.

   Note: A task may be paused only if the status of the task is running.

4. Click **Pause**.
   A confirmation box appears.

5. Click **OK** to pause the selected task.
   The selected task is paused. For information about restarting a paused task, see *Restarting a task*.

Restarting a task

Use this procedure to restart a task.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select a paused task.

   Note: A task may be restarted only if the status of the task is paused.

4. Click **Restart**.
   A confirmation box appears.

5. Click **OK** to restart the selected task.
   The selected task is restarted.

Active Tasks report elements

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

Table 14: Active Tasks Report Elements

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

Generating an active task report

Use this procedure to generate an active task report.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

4. Click **Report**.
   The **Tasks Report** page appears.
5. Click **Print** to print the report.
6. Click **Save** to save the report.

Scheduled Tasks

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

- *Exporting active alarms*

- *Exporting alarm and event history*
- *Exporting KPIs*

Viewing scheduled tasks

Use this procedure to view the scheduled tasks.

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

The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

Scheduled Tasks elements

The **Scheduled Tasks** page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. This table describes elements on the **Scheduled Tasks** page.

Table 15: Scheduled Tasks Elements

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

Editing a scheduled task

Use this procedure to edit a scheduled task.

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

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

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

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

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

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.
3. Click **Delete**.
   A confirmation box appears.
4. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

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

   The **Scheduled Tasks** page appears, and all scheduled tasks are displayed.

2. Select one or more tasks.

   Note: If no tasks are selected, all tasks matching the current filter criteria will be included in the report.

3. Click **Report**.
   The **Scheduled Tasks Report** page appears.
4. Click **Print** to print the report.
5. Click **Save** to save the report.

Chapter

4

Alarms and Events

Topics:

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

Note: Some of the alarms in this document are shared with other applications and may not appear in this particular product.

- *GLA (33100-33149).....351*

IP Front End, IPFE (5000-5999)

This section provides information and recovery procedures for IP Front End (IPFE) alarms, which range from 5000 to 5999.

5000 - IPFE Process Failure

Alarm Group: IPFE

Description: An IPFE process has stopped.

Severity: Critical

Instance: IP address of the application server

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ipfeIpfeProcessFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

5001 - IPFE Backend Unavailable

Alarm Group: IPFE

Description: The IPFE has not received any heartbeats from an application server within the heartbeat timeout interval.

Severity: Minor

Instance: IP address of the application server

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendUnavailableNotify

Recovery: If a heartbeat is received from the application server, this alarm will clear.

1. Check the status of the application servers by navigating to the **Status & Manage > Server** page.
2. Consult the application server's documentation for recovery steps.
3. If the application server si functioning, check for network connectivity issues between the IPFE and the application server.
4. Contact *My Oracle Support (MOS)* for assistance.

5002 - IPFE address configuration error

Alarm Group: IPFE

Description: The IPFE is unable to synchronize state data with its peer. This alarm can be issued for multiple reasons, including missing or invalid configurations, inability to bind a socket to the given IP address, or incompatible versions of software. The instance column provides more details when this alarm is raised. This alarm is present when the IPFE is activated but not yet configured.

Severity: Critical

Instance: One of the following strings:

- "ipfe1 and ipfe2 address both empty" - incomplete configuration
- "ipfe1 and ipfe2 address identical" - one of the addresses is incorrect
- "IPs are both local" - the two addresses correspond to the same interface on the blade
- "ipfe1 bad address" - invalid address format
- "ipfe2 bad address" - invalid address format
- "bind error" - cannot bind a socket to this interface address
- "cannot open ipfe device /dev/recent" - xt_recent module in TPD is either missing or incorrect
- "peer software version incompatible" - peer IPFE is on a different version

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeStateSyncConfigErrorNotify

Recovery: If the IPFE is able to successfully synchronize data with its peer, this alarm will clear.

1. To correct configuration errors, select **IPFE > Configuration > Options** from the left-hand menu.

   The **Configuration Options** pane appears.

2. Ensure that **IPFE1 IP Address** and **IPFE2 IP Address** are configured correctly.

3. For issues with modules or versions, contact *My Oracle Support (MOS)* for assistance.

5003 - IPFE state sync run error

Alarm Group: IPFE

Description: The IPFE was unable to synchronize state data with its mate.

Severity: Critical

Instance: One of the following strings:

- "connect error" - cannot connect to peer IPFE
- "data read error" - error reading data from peer IPFE
- "data write error" - error writing data to peer IPFE

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeStateSyncRunErrorNotify

Recovery: If the IPFE is able to synchronize state data with its mate, this alarm will clear.

1. Check the status of the peer IPFE by navigating to the **Status & Manage > Server** page.
2. If the IPFE is down, restart the process:
   a) Select **Status & Manage > Server**. The **Server Status** page appears.

b) Click to select the IPFE to restart.

c) Click **Restart**.

A warning message appears: **Are you sure you want to restart application software on the following server(s)? <server name>**.

d) Click **OK** to continue.

3. Diagnose any network fault between the two IPFEs.

4. For further assistance, contact *My Oracle Support (MOS)*.

5004 - IPFE IP tables configuration error

Alarm Group: IPFE

Description: A target set address is configured with no IP addresses, or with invalid IP addresses. This alarm can be triggered during configuration of the IPFE when the target set address has been configured, but application servers have not yet been added to the target set.

Severity: Critical

Instance: "tsa N address misconfiguration" where N is 1-16

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeIpTablesConfigErrorNotify

Recovery: When the target set address is configured correctly, this alarm will clear.

1. Select **IPFE > Configuration > Options** from the left-hand menu.

The **Configuration Options** pane appears.

2. Ensure that the **TSA1 IP Address** field contains a valid IP address.

3. Select **IPFE > Configuration > IP List TSA 1**.

The **IP List TSA 1** pane appears.

4. Ensure that there is at least one application server IP address configured for the TSA.

5. Repeat for **IPFE > Configuration > IP List TSA 1**.

5005 - IPFE Backend In Stasis

Alarm Group: IPFE

Description: The IPFE has received a heartbeat packet from the application server that indicates that the application server is unwilling to accept new connections. However, the application server will continue to process existing connections. The application server sends a stasis heartbeat message for the following reasons:

• The application server has reached its maximum number of active Diameter connections
• The application server is congested. The application server will raise *22200 - Local MP Congestion* also.

Severity: Minor

Instance: IP address of the application server in stasis

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendInStasisNotify

Recovery: When the IPFE receives heartbeats from the application server indicating that it is willing to accept new connections, this alarm will clear.

5006 - Error reading from Ethernet device. Restart IPFE process.

Alarm Group: IPFE

Description: The IPFE was unable to read from an ethernet device.

Severity: Critical

Instance: "pcap <ethernet device name>"

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfeIpfeEtherDeviceReadErrorNotify

Recovery: If the IPFE is able to read from the ethernet device, this alarm will clear.

1. Select **Status & Manage > Server**.
   The Server Status page appears.
2. Click to select the IPFE to restart.
3. Click **Restart**.

   A warning message appears:

   Are you sure you want to restart application software on the following server(s)? <server name>

4. Click **OK** to continue.

5007 - Out of Balance: Low

Alarm Group: IPFE

Description: Traffic statistics reveal that an application server is processing higher than average load. For example, if a TSA has three application servers, but the IPFE has only two connections open, then one of the application servers will receive no traffic and thus will be considered "underloaded".

Severity: Minor

Instance: IP address of the application server

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendUnderloadedNotify

Recovery: None required. Underloaded application servers do not impact traffic processing. This alarm will clear when traffic statistics reveal that the application server is no longer underloaded.

5008 - Out of Balance: High

Alarm Group: IPFE

Description: Traffic statistics reveal that an application server is processing higher than average load and will not receive new connections.

Severity: Minor

Instance: IP address of the overloaded application server

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendOverloadedNotify

Recovery: When traffic statistics indicate that the application server is no longer overloaded, this alarm will clear.

1. The IPFE will monitor traffic statistics and will not assign connections to the overloaded application server until statistics indicate that the server is no longer overloaded.
2. Check the status of the application servers by navigating to the **Status & Manage > Server** page.
3. Consult the application server's documentation for recovery steps.

5009 - No available servers in target set

Alarm Group: IPFE

Description: Through monitoring of the application servers, the IPFE learns that no server in a target set is available. The associated measurement, TxReject, will also show counts (refer to the *DSR Measurements Reference* for details about this measurement). This alarm can be triggered during configuration of the IPFE when the target set address has been configured, but application servers have not yet been added to the target set.

Severity: Critical

Instance: "tsa *N* has no available servers" where *N* is 1-16

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeNoAvailableAppServersNotify

Recovery: When at least one application server in a target set becomes available, this alarm will clear.

1. Ensure that application servers have been configured for the target set address by viewing **IPFE > Configuration > Target Sets**.
2. Check the status of the application servers by navigating to the **Status & Manage > Server** page.
3. Consult the application server's documentation for recovery steps.

4. Ensure that `ipfeNetUpdate.sh` has been run by looking for the following lines in `/etc/sysconfig/` network on the IPFE blades:

```
IPV6FORWARDING=yes
IPV6_AUTOCONF=no
```

If `ipfeNetUpdate.sh` has not bee run:

- Log in as **root.**
- At the prompt, type `ipfeNetUpdate.sh`
- At the prompt, type `init 6`
- Repeat for each IPFE blade.

5. If application servers have been configured correctly for the target set and the application server status is healthy, contact *My Oracle Support (MOS)* for assistance.

5010 - Unknown Linux iptables command error

Alarm Group: IPFE

Description: The IPFE received an unknown error parsing Linux iptables output. This is an internal software error.

Severity: Critical

Instance: "error parsing iptables output"

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeErrorParsingIptablesOutputNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

5011 - System or platform error prohibiting operation

Alarm Group: IPFE

Description: The IPFE is unable to use its ethernet interfaces. This alarm is raised during the following conditions:

- The IPFE cannot write to its Ethernet devices (denoted by the instances "Error opening ethernet listeners" or "No network cards found."
- The IPFE receives an unknown error when accessing its Ethernet devices.
- The issuances of the "Service network restart" command.
- The IPFE cannot assign Ethernet device queues to certain CPUs, which is denoted by the instance "Cannot update `/proc/irq/N/smp_affinity setting`."

Severity: Critical

Instance:

- "Error opening ethernet listeners"

- "No network cards found"
- "Cannot update `/proc/irq/N/smp_affinity setting`
- "System has less that 16 CPUs"

    Note: The IPFE detects if it has been installed on a virtual machine and will not raise this alarm.

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeSystemErrorNotify

Recovery: If the IPFE is able to use its ethernet interfaces, this alarm will clear.

1. If the IPFE is able to use its ethernet interfaces, this alarm will clear. If this alarm was generated by issuing a "service network restart" command, it should clear within 10 seconds. If it does not clear, restart the IPFE process:

    a) Select **Status & Manage > Server**. The **Server Status** page appears.
    b) Click to select the IPFE to restart.
    c) Click **Restart**.

        A warning message appears: **Are you sure you want to restart application software on the following server(s)? <server name>**.

    d) Click **OK** to continue.
    e) If the alarm still does not clear, check the Ethernet devices and CPUs.

2. Contact *My Oracle Support (MOS)* for assistance.

5012 - Signaling interface heartbeat timeout

Alarm Group: IPFE

Description: Heartbeats to monitor the liveness of a signaling interface have timed out.

Severity: Critical

Instance: The name of the Ethernet interface affected, eg. "bond0.5" etc.

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfeIpfeSignalingInterfaceNotify

Recovery:

1. Check if any manual configuration changes have been executed that remove or reset interfaces.
2. Diagnose hardware failure of interfaces, switch failure, or network outage.
3. Review currently active platform alarms.
4. If the problem persists, contact *My Oracle Support (MOS)*.

5013 - Throttling traffic

Alarm Group: IPFE

Description: IPFE has seen traffic in excess of Global Packet Rate Limit and is dropping packets in order to throttle the traffic.

Severity: Critical

Instance: The number of packets that have been throttled

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfeIpfeThrottlingTrafficNotify

Recovery:

1. Compare the setting for the **Global Packet Rate Limit** configuration found under **IPFE** > **Configuration** > **Options** with the system's performance specifications and determine if a higher setting is reasonable.
2. Review macro conditions that lead to high signal rate.
3. If the problem persists, contact *My Oracle Support (MOS)*.

5100 - Traffic overload

Alarm Group: IPFE

Description: Total IPFE signaling traffic rate is approaching or exceeding its engineered capacity. The severity thresholds are the following:

- Minor: set at 1.92 Gb/second, clear at 1.72 Gb/second
- Major: set at 2.56 Gb/second, clear at 2.36 Gb/second
- Criticalset at 3.20 Gb/second, clear at 3.00 Gb/second

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeTrafficOverloadNotify

Recovery: If the signaling traffic declines below the clear threshold, the alarm will clear.

The product is in excess of its design parameters, and may exhibit traffic loss if an additional failure occurs. Consider expanding system to accommodate additional capacity. Contact *My Oracle Support (MOS)* for assistance.

5101 - CPU Overload

Alarm Group: IPFE

Description: CPU utilization is approaching maximum levels.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ipfeIpfeCpuOverloadNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

5102 - Disk Becoming Full

Alarm Group: IPFE

Description: Disk space utilization is approaching maximum levels.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ipfeIpfeDiskUsageNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

5103 - Memory Overload

Alarm Group: IPFE

Description: IPFE memory utilization is approaching maximum levels.s

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ipfeIpfeMemoryOverloadNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

5201 - Destination port out of range

Alarm Group: IPFE

Description: The IPFE has received a packet containing a destination port that is outside both the responder port range and the initiator port range and has dropped it.

Severity: Info

Instance: Target set address that the packet was sent to

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: ipfeIpfeBadDestPortNotify

Recovery:

OAM validation should prevent a DA-MP from using an out-of-range port as a source port. Check the configuration of the peer node.

OAM (10000-10999)

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

10000 - Incompatible database version

Alarm Group: DB

Description: The database version is incompatible with the installed software database version.

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: 300

OID: tekelecIncompatibleDatabaseVersionNotify

Recovery: Contact *My Oracle Support (MOS)*.

10001 - Database backup started

Event Type: DB

Description: The database backup has started.

Severity: Info

Instance: GUI

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupStartNotify

Recovery: No action required.

10002 - Database backup completed

Event Type: DB

Description: Backup completed

Severity: Info

Instance: GUI

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupCompleteNotify

Recovery:

No action required.

10003 - Database backup failed

Event Type: DB

Description: The database backup has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupFailNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10004 - Database restoration started

Event Type: DB

Description: The database restoration has started.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreStartNotify

Recovery:

No action required.

10005 - Database restoration completed

Event Type: DB

Description: The database restoration is completed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreCompleteNotify

Recovery:

No action required.

10006 - Database restoration failed

Event Type: DB

Description: The database restoration has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreFailNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10008 - Database provisioning manually disabled

Alarm Group: DB

Description: Database provisioning has been manually disabled.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecProvisioningManuallyDisabledNotify

Recovery:

No action required.

10009 - Config and Prov db not yet synchronized

Alarm Group: REPL

Description: The configuration and the provisioning databases are not yet synchronized.

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTCfgProvDbNoSyncNotify

Recovery:

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

10010 - Stateful db from mate not yet synchronized

Alarm Group: HA

Description: The stateful database is not synchronized with the mate database.

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTStDbNoSyncNotify

Recovery:

If alarm persists for more than 30 seconds, contact *My Oracle Support (MOS)*.

10011 - Cannot monitor table

Alarm Group: OAM

Description: Monitoring for table cannot be set up.

Severity: Major

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTCantMonitorTableNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10012 - Table change responder failed

Alarm Group: OAM

Description: The responder for a monitored table failed to respond to a table change.

Severity: Major

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTResponderFailedNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10013 - Application restart in progress

Alarm Group: HA

Description: An application restart is in progress.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTApplSWDisabledNotify

Recovery:

If duration of alarm is greater than two seconds, contact *My Oracle Support (MOS)*.

10020 - Backup failure

Alarm Group: DB

Description: Database backup failed.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7ApwBackupFailureNotify

Recovery:

Alarm will clear if a backup (Automated or Manual) of the same group data is successful. Contact *My Oracle Support (MOS)* if failures persist.

10050 - Resource Audit Failure

Alarm Group: AUD

Description: Database backup failed.

Severity: Minor

Instance:

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecResourceAuditFailureNotify

Recovery:

10051 - Route Deployment Failed

Alarm Group: AUD

Description: An error occurred in the deployment of a network.

Severity: Minor

Instance: Route ID that failed to deploy

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecRouteDeploymentFailedNotify

Recovery:

   Edit the route to choose a gateway that is reachable or delete the route.

10052 - Route discovery failed

Alarm Group: AUD

Description: An error occurred in the discovery of network routes.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecRouteDiscoveryFailedNotify

Recovery:

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

10053 - Route deployment failed - no available device

Alarm Group: AUD

Description: A suitable device could not be identified for the deployment of a network route.

Severity: Minor

Instance: Route ID that failed to deploy

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecNoRouteDeviceNotify

Recovery:

1. Deploy the route on a specific device instead of using the "AUTO" device.
2. Ensure that every server in the server group has a usable device for the selected gateway.

10054 - Device deployment failed

Alarm Group: AUD

Description: An error occurred in the deployment of a network device.

Severity: Minor

Instance: Device name that failed to deploy

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecDeviceDeploymentFailedNotify

Recovery:

Edit or delete the device.

10055 - Device discovery failed

Alarm Group: AUD

Description: An error occurred in the discovery of network devices.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecDeviceDiscoveryFailedNotify

Recovery:

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

10073 - Server Group Max Allowed HA Role Warning

Alarm Group: HA

Description: The server group has received the maximum number of allowed HA role warnings

Severity: Minor

Instance: Affected Server Group name

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7OAGTSgMaxAllowedHARoleWarnNotify

Recovery:

1. Login to the SO GUI and navigate to the HA page (**Main Menu** > **Status & Manage** > **HA**).
2. Click the **Edit** button and change the Max Allowed HA role of the current Standby SOAM to *Active*.
3. If you cannot perform the HA switchover, login to the server (**Main Menu** > **Status & Manage** > **Server**).
4. Click on the Active server and press the **Restart** button to restart the server.
   HA switchover occurs.
5. Verify the switchover was successful from the Active SOAM GUI, or login to the Active and Standby SOAMs and execute the following command:

   # ha.mystate

10074 - Standby server degraded while mate server stabilizes

Alarm Group: HA

Description: The standby server has temporarily degraded while the new active server stabilizes following a switch of activity.

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7HASbyRecoveryInProgressNotify

Recovery:

No action required; the alarm clears automatically when standby server is recovered. This is part of the normal recovery process for the server that transitioned to standby as a result of a failover.

10075 - Application processes have been manually stopped

Alarm Group: HA

Description: The server is no longer providing services because application processes have been manually stopped.

Severity: Minor

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7HAMtceStopApplicationsNotify

Recovery:

If maintenance actions are complete, restart application processes on the server from the **Status & Manage** > **Servers** page by selecting the Restart Applications action for the server that raised the alarm.

Once successfully restarted the alarm will clear.

10078 - Application not restarted on standby server due to disabled failure cleanup mode

Event Type: HA

Description: The Applications on the Standby server have not been restarted after an active-to- standby transition since h_FailureCleanupMode is set to 0.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7FailureRecoveryWithoutAppRestartNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10100 - Log export started

Event Type: LOG

Description: Log files export operation has started.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportStartNotify

Recovery:

No action required.

10101 - Log export successful

Event Type: LOG

Description: The log files export operation completed successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportSuccessNotify

Recovery:

  No action required.

10102 - Log export failed

Event Type: LOG

Description: The log files export operation failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportFailedNotify

Recovery:

1. Verify the export request and try the export again.
2. If the problem persists, contact *My Oracle Support (MOS)*.

10103 - Log export already in progress

Event Type: LOG

Description: Log files export operation not run - export can only run on Active Network OAMP server.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportNotRunNotify

Recovery:

  Restart export operation after existing export completes.

10104 - Log export file transfer failed

Event Type: LOG

Description: The performance data export remote copy operation failed.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecExportXferFailedNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

10105 - Log export cancelled - user request

Event Type: LOG

Description: The log files export operation cancelled by user.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportCancelledUserNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

10106 - Log export cancelled - duplicate request

Event Type: LOG

Description: The log files export operation was cancelled because a scheduled export is queued already.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportCancelledDuplicateNotify

Recovery:

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

10107 - Log export cancelled - queue full

Event Type: LOG

Description: The log files export operation cancelled because the export queue is full.

Severity: Info

Instance: <Task ID>

Note: <Task ID> refers to the ID column found in **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks**.

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportCancelledQueueNotify

Recovery:

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

10108 - Duplicate scheduled log export task

Alarm Group: LOG

Description: A duplicate scheduled log export task has been queued.

Severity: Minor

Instance: <Target ID>

Note: <Target ID> refers to the scheduled task ID found by running a report from **Main Menu** > **Status & Manage** > **Tasks** > **Scheduled Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecLogExportDupSchedTaskNotify

Recovery:

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

10109 - Log export queue is full

Alarm Group: LOG

Description: The log export queue is full

Severity: Minor

Instance: <Queue Name>

Note: <Queue Name> refers to the name of the queue used for the export task ID found by running a report from either **Main Menu** > **Status & Manage** > **Tasks** > **Active Tasks** or **Main Menu** > **Status & Manage** > **Tasks** > **Scheduled Tasks**.

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecLogExportQueueFullNotify

Recovery:

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

10151 - Login successful

Event Type: LOG

Description: The login operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLoginSuccessNotify

Recovery:

No action required.

10152 - Login failed

Event Type: LOG

Description: The login operation failed

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLoginFailedNotify

Recovery:

Verify login information and case is correct, and re-enter.

10153 - Logout successful

Event Type: LOG

Description: The logout operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogoutSuccessNotify

Recovery:

No action required.

10154 - User Account Disabled

Alarm Group: AUTH

Description: User account has been disabled due to multiple login failures.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecAccountDisabledNotify

Recovery:

The alarm will clear if the account is automatically re-enabled. Otherwise, the administrator must enable or delete user account.

10155 - SAML Login Successful

Alarm Group: LOG

Description: SAML Login Successful

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: awpss7TekelecSamlLoginSuccessNotify

Recovery:

This is not a failure event. It's an indication that a user was successfully authenticated for login to the GUI. This applies to both conventional login and Single Sign On (SSO) login.

10156 - SAML Login Failed

Alarm Group: LOG

Description: An attempt to login to the GUI via conventional login or via SSO login failed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: awpss7TekelecSamlLoginFailedNotify

Recovery:

1. Use correct username and password to log in.
2. For failed SSO login, verify SSO was properly configured. Collect logs and contact *My Oracle Support (MOS)* if the problem persists.

10200 - Remote database reinitialization in progress

Alarm Group: CFG

Description: The remote database reinitialization is in progress. This alarm is raised on the active NOAMP server for the server being added to the server group.

Severity: Minor

Instance: <hostname of remote server>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7ApwSgDbReinitNotify

Recovery:

1. Check to see that the remote server is configured.
2. Make sure the remote server is responding to network connections.
3. If this does not clear the alarm, delete this server from the server group.
4. If the problem persists, contact *My Oracle Support (MOS)*.

IDIH (11500-11549)

This section provides information and recovery procedures for IDIH alarms, which range from 11500 to 11549.

11500 - Tracing Suspended

Alarm Group: IDIH

Description: IDIH trace has been suspended due to DA-MP (danger of) CPU congestion.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterTracingSuspendedAlarmNotify

Recovery:

   No action required

11501 - Trace Throttling Active

Alarm Group: IDIH

Description: Troubleshooting trace has been throttled on some MPs due to IDIH TTR bandwidth usage exceeding provisioned limit.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterTracingThrottledAlarmNotify

Recovery:

   No action required

11502 - Troubleshooting Trace Started

Event Group: IDIH

Description: A troubleshooting trace instance was started.

Severity: Info

Instance: <TraceInstanceId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterIDIHTraceStartedNotify

Recovery:

No action required.

11503 - Troubleshooting Trace Stopped

Event Group: IDIH

Description: A troubleshooting trace instance was stopped.

Severity: Info

Instance: <TraceInstanceId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterIDIHTraceStoppedNotify

Recovery:

No action required

11504 - Invalid DIH IP Address

Alarm Group: IDIH

Description: Unable to connect via ComAgent to remote DIH server with IP

Severity: Minor

Instance: String of Configured DIH IP Address

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterInvalidDihIpAddressAlarmNotify

Recovery:

No action required

Session Binding Repository, SBR (12000-12010)

This section provides information and recovery procedures for SBR alarms, which range from 12000 to 12999.

12003 - SBR Congestion State

Alarm Group: SBRA

Description: The SBR application is in a congested state and is shedding operations. The measurement Sbr.RxIngressMsgQueueAvg shows the average percentage of queue length utilization, which is used to determine congestion. The severity thresholds are the following:

Table 16: Congestion Thresholds

Severity	Set Threshold	Clear Threshold	Shed Operations	Associated Measurements
Minor	60%	50%	Creates	Sbr.TxShedCreates
Major	80%	70%	Creates, Writes	Sbr.TxShedCreates Sbr.TxShedWrites
Critical	95%	90%	Creates, Writes, Reads	Sbr.TxShedCreates Sbr.TxShedWrites Sbr.TxShedReads

Note: Refer to the *DSR Measurements Reference* for details about these measurements.

Severity: Minor, Major, Critical

Instance: Sbr.RxIngressMsgQueueMetric[subId], SBR

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeSbrCongestionStateNotify

Recovery: If congestion falls below the clear threshold, this alarm will clear.

The SBR congestion status exceeds the alarm threshold. Additional capacity may be required to service the traffic load. Contact *My Oracle Support (MOS)* for assistance.

12007 - SBR Active Sess Binding Threshold

Alarm Group: SBRA

Description: The SBR application has exceeded its Active Session Binding threshold. The configuration, **Maximum active session bindings**, is used to calculate the percentage. The severity thresholds are the following:

- Minor: set at 70%, clear at 60%
- Major: set at 80%, clear at 70%
- Critical: set at 100%, clear at 90%

Severity: Minor, Major, Critical

Instance: Sbr.EvCurrentSessionMetric, SBR

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeSbrActiveSessBindThresholdNotify

Recovery: If total active session bindings fall below the clear threshold, this alarm will clear.

1. Select **CPA** > **Configuration** > **SBR**.

   The **CPA** > **Configuration** > **SBR** page appears.

2. Increase the **Maximum active session bindings** configuration if it is too low.

3. Click **Apply** to apply your changes.

   Your changes will go into affect immediately.

4. The SBR active session bindings count exceeds the threshold. Additional capacity may be required to service the traffic load. Contact *My Oracle Support (MOS)* for assistance.

12010 - SBR Proc Term

Alarm Group: SBRA

Description: The SBR application has terminated.

Severity: Critical

Instance: sbr

HA Score: Degraded

Auto Clear Seconds: 10

OID: ipfeSbrProcTermNotify

Recovery: When an active SBR is terminated as indicated by this alarm, its standby becomes active. The Process Manager will automatically attempt to restart the terminated process. If the Process Manager fails to start the terminated process, it will raise the alarm again. The standby that became active will remain active until it is placed into standby mode again.

1. Check the status of the terminated SBR by navigating to the **Status & Manage > Server** page.

2. If the Process Manager cannot restart the process, contact *My Oracle Support (MOS)* for assistance.

SS7/Sigtran Alarms (19200-19299)

This section provides information and recovery procedures for SS7/Sigtran alarms, ranging from 19200 - 19299.

19200 - RSP/Destination unavailable

Alarm Group: SS7

Description: Unable to access the SS7 Destination Point Code because the RSP status is Unavailable.

Severity: Critical

Instance: RSP Name

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlRspUnavailableNotify

Recovery:

1. RSP/Destination status can be monitored from the SOAM GUI **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.

    - If the RSP/Destination becomes Unavailable due to a link set failure, the MP server will attempt to automatically recover all links not manually disabled.
    - If the RSP/Destination becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.

2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

19201 - RSP/Destination route unavailable

Alarm Group: SS7

Description: Unable to access the SS7 Destination point code via this route.

Severity: Minor

Instance: <Route Name>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlRouteUnavailableNotify

Recovery:

1. Route status can be monitored from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.

    - If the route becomes Unavailable due to a link set failure, the MP server will attempt to automatically recover all links not manually disabled.
    - If the route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.

2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

19202 - Linkset unavailable

Alarm Group: SS7

Description: The SS7 link set to an adjacent signaling point has failed.

Severity: Major

Instance: <LinkSetName>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlLinksetUnavailableNotify

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link set status can be monitored from **SS7/Sigtran** > **Maintenance** > **Linksets**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact *My Oracle Support (MOS)*.

19203 - Link unavailable

Alarm Group: SS7

Description: M3UA has reported to M3RL that a link is out of service.

Severity: Minor

Instance: <Link Name>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlLinkUnavailableNotify

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link status can be monitored from **SS7/Sigtran** > **Maintenance** > **Links**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact *My Oracle Support (MOS)*.

19204 - Preferred route unavailable

Alarm Group: SS7

Description: M3RL has started to utilize a lower priority (higher cost) route to route traffic toward a given destination address, because the higher priority (lower cost) route specified for that RSP/Destination has become Unavailable.

Severity: Major

Instance: RSP Name

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlPreferredRouteUnavailableNotify

Recovery:

1. If the preferred route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Route status can be monitored from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.
3. Verify that IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. If the problem persists, contact *My Oracle Support (MOS)*.

19205 - TFP received

Event Type: SS7

Description: The TFP message was received by M3RL layer; an adjacent point code has reported that it has no longer has any available routes to the RSP/Destination.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7M3rlTfpReceivedNotify

Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.
2. Follow local procedures to determine the reason that the PC was prohibited.

19206 - TFA received

Event Type: SS7

Description: TFA message received by M3RL layer; an adjacent point code has reported that it has an available route to the RSP/Destination.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7M3rlTfaReceivedNotify

Recovery:

Monitor the RSP/Destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.

19207 - TFR received

Event Type: SS7

Description: TFR message received by M3RL layer; an adjacent point code has reported that an available route to the RSP/Destination has a restriction/limitation.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7M3rlTfrReceivedNotify

Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.
2. Follow local procedures to determine the reason that the PC was prohibited.

19208 - TFC received

Event Type: SS7

Description: TFC message received by M3RL layer; an adjacent or non-adjacent point code is reporting the congestion level of a RSP/Destination.

Severity: Info

HA Score: Normal

Throttle Seconds: 30

Instance: N/A

OID: awpss7M3rlTfcReceivedNotify

Recovery:

1. RSP/Destination status can be monitored from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.
2. Follow local procedures to determine the reason that the PC was prohibited.

19209 - M3RL routing error - invalid DPC

Event Type: SS7

Description: A message was discarded due to a routing error.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 10

OID: awpss7M3rlRoutingFailureNotify

Recovery:

1. Each MP's assigned point code can be monitored from **SS7/Sigtran** > **Configuration** > **Local Signaling Points**.
2. If the event was caused by:
   - The DPC of an egress message is not configured as a remote signaling point, then look at the routing label in the event additional information, determine the DPC, and verify that the DPC is configured as an RSP.
   - The DPC of an egress message is configured but not available for routing, then look at the routing label in the event additional information, determine the DPC, verify that a route exists for the DPC, and use the RSP status screen to verify that a route is available for the RSP.
   - The DPC of an ingress message does not match the TPC or CPC of the MP server group, then either signaling is being misdirected by the STP toward the MP, or the MP server's LSP is misconfigured. Look at the routing label in the event additional information for the OPC and DPC of the ingress message.

3. If a high number of these errors occurs, then an internal routing table problem may exist. Please contact *My Oracle Support (MOS)* for assistance.

19210 - M3RL routing error - invalid NI

Event Type: SS7

Description: The message was discarded due to a routing error. The NI (Network Indicator) value received in a message from the network is not assigned to the MP. This event is generated under the following circumstances:

- The NI in the MTP3 routing label of the ingress message is not supported for the given network signaling domain for a provisioned Local Signaling Point.
- For an ingress ANSI SCCP message, Bit-8 in the SCCP CDPA address indicator octet indicates that the CDPA is encoded as per international specifications:
  - A "0" in Bit 8 indicates that the address is international and that both the address indicator and the address are coded according to international specifications.
  - A "1" in Bit 8 indicates that the address is national and that both the address indicator and the address are coded according to national specifications.

    The NI cannot be International for ANSI messages, since the ordering of the subsystem number indicator field and the point code indicator fields are in the reverse order in the ITU specification.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 10

OID: awpss7M3rlRoutingFailureInvalidNiNotify

Recovery:

1. The Signaling Transfer Point or Signaling Gateway routing tables may be inconsistent with the NI assigned to the MP. You can monitor each MP's assigned NI value from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Remote Signaling Points**.
2. If the problem persists, contact *My Oracle Support (MOS)*.

19211 - M3RL routing error - invalid SI

Event Type: SS7

Description: The message was discarded due to a routing error. The SI value received in a message from the network is associated with a User Part that is not currently supported.

Severity: Info

Instance: RSP Name

HA Score: Normal

Throttle Seconds: 10

OID: awpss7M3rlRoutingFailureInvalidSiNotify

Recovery:

1. If the SI received is not a **0** (SNM) or **3** (SCCP), verify that the STP/SG and the point code that created the message have correct routing information.
2. If the problem persists, contact *My Oracle Support (MOS)*.

19217 - Node isolated - all links down

Alarm Group: SS7

Description: All configured links are down; either failed or disabled. No M3UA signaling is possible. The node is isolated from the network. All M3UA connectivity to the SS7/Sigtran network has either failed or has been manually disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlNodeIsolatedAllLinkDownNotify

Recovery:

1. Select **SS7/Sigtran** > **Maintenance** > **Links** to check whether any of the links are manually disabled that should not be. If so, click **Enable** to enable the manually disabled links.

2. View the active alarms and event history logs by selecting **Alarms & Events** > **View Active** and **Alarms & Events** > **View History**. Look for significant events that may affect the IP network, associations, or links.

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

19226 - Timedout waiting for ASP-UP-ACK

Event Type: SS7

Description: When an association is in the **Enabled** administrative state, part of the association initialization involves sending an ASP-UP from the MP server and receiving an ASP-UP-ACK from the adjacent server. If ASP-UP is sent, but no ASP-UP-ACK is received within State Management ACK Timer milliseconds, this event is generated and the ASP-UP is attempted again. ASP-UP attempts will continue indefinitely until the association administrative state is set to **Blocked** or **Disabled**, or the SCTP transport fails, or the ASP-UP-ACK is received.

Severity: Info

Instance: <AssocName>

HA Score: Normal

Throttle Seconds: 10

OID: awpss7TimedOutWaitingForAspUpAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. Verify that the timer value for State Management ACK Timer is not set too short to allow the adjacent server to respond with an ASP-UP-ACK. This should be rare if the network is not congested.
3. If the problem persists, contact *My Oracle Support (MOS)*.

19227 - Received unsolicited ASP-DOWN-ACK

Event Type: SS7

Description: The adjacent server at the specified IP address and port has sent an ASP-DOWN-ACK, but not in response to an ASP-DOWN message from the MP server. Normally this indicates that the far-end of the association is being taken down for maintenance. If the association administrative state is **Enabled**, the MP server will automatically attempt to bring the association back to ASP-UP. This is done by sending an ASP-UP. The MP server will continue to send ASP-UP until an ASP-UP-ACK is received, the SCTP association comes down, or the association administrative state is changed to **Blocked** or **Disabled**.

Severity: Info

Instance: <AssocName>

HA Score: Normal

Throttle Seconds: 30

OID: awpss7ReceivedUnsolicitedAspDownAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. If the problem persists, contact *My Oracle Support (MOS)*.

19229 - Timed out waiting for ASP-ACTIVE-ACK

Event Type: SS7

Description: No ASP-ACTIVE-ACK is received in response to an ASP-ACTIVE message on the link within State Management ACK Timer milliseconds.

Severity: Info

Instance: <LinkName>

HA Score: Normal

Throttle Seconds: 10

OID: awpss7TimedOutWaitingForAspActiveAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. Verify that the timer value for State Management ACK Timer is not set too short to allow the adjacent server to respond with an ASP-ACTIVE-ACK. This should be rare if the network is not congested.
3. If the problem persists, contact *My Oracle Support (MOS)*.

19230 - Received unsolicited ASP-INACTIVE-ACK

Event Type: SS7

Description: An unsolicited ASP-INACTIVE-ACK is received on the link.

Severity: Info

Instance: <LinkName>

HA Score: Normal

Throttle Seconds: 10

OID: awpss7ReceivedUnsolicitedAspInactiveAckNotify

Recovery:

1. Verify that the adjacent server on the signaling gateway is not under maintenance.
2. If the problem persists, contact *My Oracle Support (MOS)*.

19231 - Received invalid M3UA message

Event Type: SS7

Description: The far-end has sent an invalid M3UA message to which the MP server has responded with an M3UA ERROR message.

Severity: Info

Instance: <LinkName> or <AssocName> Information about the type of error and the accompanying diagnostic data is included in the event additional information.

HA Score: Normal

Throttle Seconds: 10

OID: awpss7ReceivedInvalidM3uaMessageNotify

Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the malformed message.

   - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
   - Error code 0x03 indicates an unsupported M3UA message class.
   - Error code 0x04 indicates an unsupported M3UA message type.
   - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
   - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
   - Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
   - Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
   - Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
   - Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.

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

19233 - Failed to send non-DATA message

Event Type: SS7

Description: An attempt to send an M3UA non-DATA message has failed. Non-DATA messages include SSNM, ASPSM, ASPTM, and MGMT messages. The message has been discarded. Possible reasons for the failure include:

- The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing the MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
- The socket has closed just as the send was being processed.

Severity: Info

Instance: <LinkName> or <AssocName>

Note: Information about the type of error and the accompanying diagnostic data is included in the event additional information.

HA Score: Normal

Throttle Seconds: 10

OID: awpss7FailedToSendNonDataMessageNotify

Recovery:

1. Select **Alarms & Events** > **View History** and check the event history logs for additional SS7 events or alarms from this MP server.
2. Verify that the adjacent server on the signaling gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.
3. If the problem persists, contact *My Oracle Support (MOS)*.

19234 - Local link maintenance state change

Event Type: SS7

Description: The link administrative state is manually changed from one administrative state to another.

Severity: Info

Instance: <LinkName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awpss7LocalLinkMaintenanceStateChangeNotify

Recovery:

1. No action required if this was an expected change due to some maintenance activity. Otherwise, security logs can be examined on the SOAM server to determine which user changed the administrative state.
2. If the problem persists, contact *My Oracle Support (MOS)*.

19235 - Received M3UA error

Event Type: SS7

Description: An M3UA ERROR message is received from the adjacent server.

Severity: Info

Instance: <LinkName> or <AssocName>

Note: Information about the type of error and the accompanying diagnostic data is included in the event additional information.

HA Score: Normal

Throttle Seconds: 10

OID: awpss7ReceivedM3uaErrorNotify

Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the ERROR message.

   • Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.

- Error code 0x03 indicates an unsupported M3UA message class.
- Error code 0x04 indicates an unsupported M3UA message type.
- Error code 0x05 indicates an unsupported M3UA traffic mode.
- Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
- Error code 0x09 indicates an invalid SCTP stream identifier. A DATA message was sent on stream 0.
- Error code 0x0D indicates that the message was refused due to management blocking. An ASP Up or ASP Active message was received, but refused for management reasons.
- Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
- Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
- Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
- Error code 0x14 indicates that the destination status is unknown. This message can be sent in response to a DAUD from the MP server if the SG cannot or does not wish to provide the destination status or congestion information.
- Error Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
- Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.

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

19240 - Remote SCCP subsystem prohibited

Alarm Group: SS7

Description: The status of remote SCCP subsystem has changed to **Prohibited**.

Severity: Minor

Instance: <RMU>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7RemoteSccpSubsystemProhibitedNotify

Recovery:

1. You can monitor destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points** and RMU/subsystem status from **SS7/Sigtran** > **Maintenance** > **Remote MTP3 Users**.

   - If the subsystem's status changed to **Prohibited** because SCMG received a SSP message, an audit of the status of the RMU via the SCCP subsystem status test (SST) procedure is performed.
   - If the subsystem's status changed to **Prohibited** because SCCP received a MTP-PAUSE indication from M3RL, then recovery actions of restoring the RSP/Destination status to **Available** will be invoked by M3RL.

- If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS `cause=unequipped user` indication from M3RL, then no automatic recovery will be initiated. Only manual action at the remote node can correct a remote point code that has not been configured with SCCP.
- If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS `cause=unknown` or `inaccessible` indication from M3RL, then SCCP will automatically invoke subsystem status testing depending upon the network type:
  - ANSI: subsystem status testing of all RMUs associated with the point code.
  - ITU: subsystem status testing SCMG (`SSN=1`) associated with the point code.

2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Select **Alarms & Events** > **View History** and check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. Follow local procedures to determine the reason that the far-end SSN is down. If it is not down, but it continues to be reported as down, contact *My Oracle Support (MOS)*.

19241 - SCCP message type unrecognizedSCCP malformed or unsupported message

Event Type: SS7

Description: SCCP discarded an ingress message because the Message Type is not currently supported. The following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. The following SCMG Message Types are supported: SSA, SSP, and SST.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpMsgTypeUnrecognizedNotify

Recovery:

1. Investigate:
   - If the originator of the message is misconfigured.
   - If the network is misconfigured, causing messages to be routed to the wrong RSP/Destination.
   - If the message type is currently unsupported.

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

19242 - SCCP Hop counter violation

Event Type: SS7

Description: SCCP discarded an ingress message because a Hop Counter violation was detected.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpHopCounterViolationNotify

Recovery:

1. One of the following conditions causes this error:

   • The originator of the message is setting the initial value too low.
   • The message is being rerouted too many times by the STPs, possibly because of an STP routing misconfiguration that has caused message looping.

2. Contact *My Oracle Support (MOS)*.

19243 - SCCP routing failure

Event Type: SS7

Description: SCCP was unable to route or process a UDT or XUDT message during SCCP processing for reasons (other than a global title translation failure, detected SCCP loop) possibly requiring operator intervention.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpRoutingFailureNotify

Recovery:

1. These failures are typically associated with invalid information received in the SCCP messages. Check for the following:

   • A misconfiguration of the SCCP at the originating or terminating node
   • Network routing misconfiguration at the STPs

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

19244 - SCCP routing failure network status

Event Type: SS7

Description: SCCP was unable to route or process a UDT or XUDT message during SCCP processing due to transient conditions such as RSP/destination failures and remote or local subsystem failures.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpRoutingFailureNetworkStatusNotify

Recovery:

1. Typically these routing failures occur due to transient conditions such as RSP/Destination and Subsystem failures. Destination status can be monitored from the SOAM GUI **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points** and RMU/Subsystem status can be monitored from **SS7/Sigtran** > **Maintenance** > **Remote MTP3 Users**.

2. Monitor status on the GUI main menu as follows:

   - Destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.
   - RMU/subsystem status from **SS7/Sigtran** > **Configuration** > **Remote MTP3 Users**.
   - Local subsystem status from **SS7/Sigtran** > **Maintenance** > **Local SCCP Users**.

3. Verify that IP network connectivity exists between the MP server and the adjacent servers.

4. Check the event history logs for additional SS7 events or alarms from this MP server.

5. Verify that the adjacent server is not under maintenance.

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

19245 - SCCP GTT failure

Event Type: SS7

Description: SCCP Global Title Translation has failed to determine a destination for a PDU. SCCP is invoking the message return procedure.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 10

OID: awpss7SccpGttFailureNotify

Recovery:

1. Global title translation has failed. For the cause of the failure, look at the SCCP return cause and the called party address information in the event additional information field. Look for the following items:

   - Missing global title translation data.
   - Incorrect called party address information in the ingress message.
   - Point code paused or congested.
   - Subsystem prohibited or congested.

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

19246 - Local SCCP subsystem prohibited

Alarm Group: SS7

Description: The status of the local SCCP subsystem has changed to **Prohibited**. This alarm is raised for one of the following conditions:

- When a new local SSN is configured and is in the disabled state.

- When a GUI maintenance operation is performed to disable the state of the local SSN.·
- On a system restart where the local SSN was is disabled state prior to the system restart.

Severity: Major

Instance: <LSP>, <SSN>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7SCCPLocalSubsystemProhibitedNotify

Recovery:

> To clear the alarm:
> a) On the SOAM GUI main menu, select **SS7/Sigtran** > **Configuration** > **Local SCCP Users**.
> b) Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
> c) Click **Enable** to put the appropriate local SSN in the enabled state.
>   A confirmation message appears.
> d) Click **OK**.
>   The **Enable** link will be grayed out once the SSN transitions to the enabled state.

19248 - SCCP Segmentation Failure

Event Type: SS7

Description: SCCP Segmentation Procedure Failure

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpSegmentationFailureNotify

Recovery:

1. This condition indicates segmentation procedure failure at the SCCP layer:
   - User data exceeds maximum size
   - Internal Error

2. Check the SCCP options configuration and maximum size limitations for the SS7 network.
3. Contact the *My Oracle Support (MOS)* for assistance.

19249 - SCCP Reassembly Failure

Event Type: SS7

Description: SCCP Segmentation Procedure Failure

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 30

OID: awpss7SccpReassemblyFailureNotify

Recovery:

1. This condition indicates reassembly procedure failure at the SCCP layer:

    *   Reassembly time expired
    *   Out of sequence segments
    *   Internal error

2. Determine if the problem is a result of routing decision errors or latency from the SS7 network.
3. Contact the *My Oracle Support (MOS)* for assistance.

19250 - SS7 process CPU utilization

Alarm Group: SS7

Description: The SS7 process, which is responsible for handling all SS7 traffic, is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, or Critical as shown in the GUI under **Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7Ss7ProcessCpuUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage** > **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The SS7 process may be experiencing problems. You monitor the alarm log from **Alarms & Events** > **View Active**.
5. If the problem persists, contact *My Oracle Support (MOS)*.

19251 - Ingress message rate

Alarm Group: SS7

Description: The ingress message rate (messages per second) for the MP is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical as shown in the GUI under**Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7IngressMsgRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage** > **Server**

2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from**Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

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

19252 - PDU buffer pool utilization

Alarm Group: SS7

Description: The percent utilization of the MP's PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded.

Severity: Minor, Major, Critical as shown in the GUI under**Alarms & Events** > **View Active**.

Instance: <PoolName> Values: ANSI, ITUI, ITUN

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7PduBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from the GUI main menu under **Status & Manage** > **Server**.

2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load.You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

4. A software defect may exist resulting in PDU buffers not being de-allocated to the pool when a PDU is successfully transmitted into the network. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log from **Alarms & Events** > **View Active**.

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

19253 - SCCP stack event queue utilization

Alarm Group: SS7

Description: The percent utilization of the MP's SCCP stack event queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7SccpStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage** > **Server**.

2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

4. If no additional congestion alarms are asserted, the SCCP Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log under **Alarms & Events** > **View Active**.

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

19254 - M3RL stack event queue utilization

Alarm Group: SS7

Description: The percent utilization of the MP's M3RL Stack Event Queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under**Status & Manage** > **Server**.

2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

4. If no additional congestion alarms are asserted, the M3RL Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events** > **View Active**.

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

19255 - M3RL network management event queue utilization

Alarm Group: SS7

Description: The percent utilization of the MP's M3RL Network Management Event Queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3rlNetMgmtEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage** > **Server**.

2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP under **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP under **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

4. If no additional congestion alarms are asserted, the M3RL Network Management Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events** > **View Active**.

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

19256 - M3UA stack event queue utilization

Alarm Group: SS7

Description: The percent utilization of the MP's M3UA Stack Event Queue is approaching its maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7M3uaStackEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage** > **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3UA Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events** > **View Active**.
5. If the problem persists, contact *My Oracle Support (MOS)*.

19258 - SCTP Aggregate Egress queue utilization

Alarm Group: SS7

Description: The percent utilization of events queued to all SCTP associations on the MP server is approaching maximum capacity.

Severity: Minor, Major, Critical as shown in the GUI under **Alarms & Events** > **View Active**.

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7SctpAggregateAssocWriteQueueUtilNotify

Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events** > **View Active**.

3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from the GUI main menu under **Status & Manage>Server**.

4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

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

19259 - Operation discarded due to local resource limitation

Event Type: SS7

Description: Operation discarded due to local resource limitation

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapOpDiscardedLocalResLimitNotify

Recovery:

1. Determine if this condition indicates a software problem or unexpected TC User behavior.

2. Contact *My Oracle Support (MOS)* for assistance if needed.

19260 - Transaction could not be delivered to remote TCAP peer due to conditions in the network

Event Type: SS7

Description: Transaction could not be delivered to remote TCAP peer due to conditions in the network.

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapTransNotDeliveredToPeerNotify

Recovery:

1. This event indicates that an SCCP service message (UDTS or XUDTS) was received from the network, meaning that the TCAP message could not be delivered to the remote TCAP peer. The event additional information field contains the first 80 octets of the SS7 message starting with the MTP3 routing label. This data can be used to determine the routing instructions for the message.

2. Verify that the routing is configured correctly for the destination. if the routing configuration is correct, determine why the remote TCAP peer is not available.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

19262 - Operation discarded due to malformed component received from remote TCAP peer

Event Type: SS7

Description: Operation discarded due to malformed component received from remote TCAP peer

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapMalformedComponentFromRemoteNotify

Recovery:

1. This event indicates that a TCAP component was received from the remote TCAP peer that could not be successfully decoded.
2. The event additional information field includes the reason why the decoding failed, plus the first 80 octets of the message starting with the MTP3 routing label. The message data can be used to determine the source of the malformed message
3. Contact *My Oracle Support (MOS)* for assistance if needed.

19263 - Transaction discarded due to malformed dialogue message received from local TC User

Event Type: SS7

Description: Transaction discarded due to malformed dialogue message received from local TC User

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapMalformedDialogueFromLocalNotify

Recovery:

1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. Contact *My Oracle Support (MOS)* for assistance if needed.

19264 - Transaction discarded due to malformed dialogue message from remote TCAP peer

Event Type: SS7

Description: Transaction discarded due to malformed dialogue message received from local TC User

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapMalformedDialogueFromRemoteNotify

Recovery:

1. This event indicates that a TCAP message was received from the remote TCAP peer that could not be successfully decoded.
2. The event additional information field includes the reason why the decoding failed, plus the first 80 octets of the message starting with the MTP3 routing label. The message data can be used to determine the source of the malformed message.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

19265 - Unexpected event received from local TC User

Event Type: SS7

Description: Unexpected event received from local TC User.

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapUnexpectedMsgFromLocalNotify

Recovery:

1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. The event additional information field includes a description of what event was received and why it was unexpected, as well as what was done with the operation or dialogue as a result.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

19266 - Unexpected event received from remote TCAP peer

Event Type: SS7

Description: Unexpected event received from remote TCAP peer

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapUnexpectedMsgFromRemoteNotify

Recovery:

1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. The event additional information field includes:

   - a description of what event was received and why it was unexpected
   - what was done with the operation or dialogue as a result
   - the first 80 octets of the message starting with the MTP3 routing label

3. The message data can be used to determine the source of the malformed message.
4. Contact *My Oracle Support (MOS)* for assistance if needed.

19267 - Dialogue removed by dialogue cleanup timer

Event Type: SS7

Description: Dialogue removed by dialogue cleanup timer

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapDialogueRemovedTimerExpiryNotify

Recovery:

1. This event indicates that a TCAP transaction containing no components was sent, but no response was received from the remote TCAP peer.
2. The event additional information field includes:

   - the local dialogue-id
   - the number of milliseconds that elapsed between the time the message was sent and the time that the message was discarded
   - the destination point code to which the message was destined
   - the SCCP called party address to which the message was destined

3. Check for SCCP events just prior to this event indicating that a message could not be routed. If SCCP failed to route the message, verify that a route exists for the destination to which the TCAP message was being sent.
4. If no SCCP routing failure event exists, investigate why the remote TCAP peer failed to respond. The DPC and called party address can be used to determine the destination to which the message was being sent.
5. Contact *My Oracle Support (MOS)* for assistance if needed.

19268 - Operation removed by invocation timer expiry

Event Type: SS7

Description: Operation removed by invocation timer expiry

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapOperationRemovedTimerExpiryNotify

Recovery:

1. This event indicates that a TCAP transaction containing no components was sent, but no response was received from the remote TCAP peer.
2. The event additional information field includes:
   - the local dialogue-id and invoke-id
   - the number of milliseconds that elapsed between the time the message was sent and the time that the operation was discarded
   - the destination point code to which the message was destined if the component was ever sent
   - the SCCP called party address to which the message was destined if the component was ever sent

3. Check for SCCP events just prior to this event indicating that a message could not be routed. If SCCP failed to route the message, verify that a route exists for the destination to which the TCAP message was being sent.
4. If no SCCP routing failure event exists, investigate why the remote TCAP peer failed to respond. The DPC and called party address (if present) can be used to determine the destination to which the message was being sent.
5. If the DPC and Called Party Address are not included in the additional information field, it indicates that the component was created, but never sent.
6. Contact *My Oracle Support (MOS)* for assistance if needed.

19269 - Dialogue aborted by remote TCAP peer

Event Type: SS7

Description: Dialogue aborted by remote TCAP peer

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapDialogueAbortByRemoteNotify

Recovery:

1. This event indicates that a remote TCAP peer has aborted a dialogue.
2. The event additional information field includes:

   - the abort reason
   - the first 80 octets of the message starting with the MTP3 routing label

3. The message data can be used to determine the source of the U-Abort or P-Abort message.
4. Contact *My Oracle Support (MOS)* for assistance if needed.

19270 - Received unsupported TCAP message

Event Type: SS7

Description: Received unsupported TCAP message

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapUnsupportedTCAPMsgRcvdNotify

Recovery:

1. This event indicates that an unsupported TCAP message has been received.
2. The event additional information field includes:

   - the abort reason
   - the first 80 octets of the message starting with the MTP3 routing label

3. The message data can be used to determine the source of the unsupported message.
4. Contact *My Oracle Support (MOS)* for assistance if needed.

19271 - Operation rejected by remote TCAP peer

Event Type: SS7

Description: Operation rejected by remote TCAP peer

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapReturnRejectByRemoteNotify

Recovery:

1. This event indicates that a remote TCAP peer has rejected an operation.
2. The event additional information field includes:

   - the reject reason

- the first 80 octets of the message starting with the MTP3 routing label

3. The message data can be used to determine the source of the message.

4. Contact *My Oracle Support (MOS)* for assistance if needed.

19272 - TCAP active dialogue utilization

Alarm Group: SS7

Description: TCAP active dialogue utilization

Severity: Minor, Major, Critical

Instance: Application name

HA Score: Normal

Auto Clear Seconds: 0 (alarm doesn't auto-clear)

OID: awpss7TcapActiveDialogueUtilNotify

Recovery:

1. The percent utilization of the MP's dialogue table is approaching maximum capacity. This alarm indicates that the number of active dialogues on the MP server is higher than expected.

2. If this problem persists and the dialogue table reaches 100% utilization, all new messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This condition may be caused by any of the following:

    - the incoming plus outgoing rate of new dialogues is higher than expected (possibly due to poor load balancing across MP servers, or too few MP servers to handle the load)
    - the duration of the dialogues is longer than expected
    - both the rate and duration are higher than expected
    - a software problem is preventing removal of completed dialogues

3. Contact *My Oracle Support (MOS)* for assistance if needed.

19273 - TCAP active operation utilization

Alarm Group: SS7

Description: TCAP active operation utilization

Severity: Minor, Major, Critical

Instance: Application name

HA Score: Normal

Auto Clear Seconds: 0 (alarm doesn't auto-clear)

OID: awpss7TcapActiveOperationUtilNotify

Recovery:

1. The percent utilization of the MP's component table is approaching maximum capacity. This alarm indicates that the number of active egress TCAP operations on the MP server is higher than expected.

2. If this problem persists and the component table reaches 100% utilization, all new egress operations will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This may be caused by any of the following:

   - the outgoing rate of new operations is higher than expected (possibly due to a higher than expected average number of operations per message)
   - the duration of the operations is longer than expected
   - both the outgoing rate and duration are higher than expected
   - a software problem is preventing removal of components

3. Contact *My Oracle Support (MOS)* for assistance if needed.

19274 - TCAP stack event queue utilization

Alarm Group: SS7

Description: TCAP stack event queue utilization

Severity: Minor, Major, Critical

Instance: Application name

HA Score: Normal

Auto Clear Seconds: 0 (alarm doesn't auto-clear)

OID: awpss7TcapStackEventQueueUtilNotify

Recovery:

1. The percent utilization of the MP's TCAP Stack Event Queue is approaching its maximum capacity. This alarm indicates that the number of ingress TCAP messages on the MP server is higher than expected.

2. If this problem persists and the queue reaches 100% utilization, all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This may be caused by any of the following:

   - the incoming rate of new TCAP messages is higher than expected (possibly due to poor load balancing across MP servers, or too few MP servers to handle the load)
   - a software problem is causing the messages to be processed more slowly than expected

3. Contact *My Oracle Support (MOS)* for assistance if needed.

19275 - Return error from remote TCAP peer

Event Type: SS7

Description: Return error from remote TCAP peer

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 30

OID: awpss7TcapReturnErrorFromRemoteNotify

Recovery:

1. This event indicates that a remote TCAP peer has responded to an operation using Return Error.
2. The event additional information field includes:

   - the error reason
   - the first 80 octets of the message starting with the MTP3 routing label

3. The message data can be used to determine the source of the message.
4. Contact *My Oracle Support (MOS)* for assistance if needed.

19276 - SCCP Egress Message Rate

Alarm Group: SS7

Description: The SCCP Egress Message Rate (Message per second) for the MP is approaching or exceeding its engineered traffic handling capacity

Severity: Major

Instance: Application name

HA Score: Normal

Auto Clear Seconds: 0 (alarm doesn't auto-clear)

OID: awpss7SccpEgressMsgRateNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance if needed.

19281 - TCAP Routing Failure

Event Type: SS7

Description: TCAP was unable to route message due to transient condition such as destination failure or destination unavailability

Severity: Info

Instance: Application name

HA Score: Normal

Throttle Seconds: 10

OID: awpss7TcapRoutingFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance if needed.

Transport Manager Alarms and Events (19400-19499)

This section provides information and recovery procedures for alarms and events, ranging from 19400-19499.

19400 - Transport Down

Alarm Group: TMF

Description: Transport Down

Severity: Major

Instance: <TransportName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: awptransmgrTransportDownNotify

Recovery:

1. The Active alarm instance data, which can be viewed from **Main Menu** > **Alarms & Events** > **View Active**, contains the Transport Name as configured in **Main Menu** > **Transport Manager** > **Configuration** > **Transport**

   Additional Information for the alarm can be found in **Main Menu** > **Alarms & Events** > **View Active or View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column. This column will include the local and remote IP addresses and ports, the administrative state, and the protocol state of the association.

   This alarm is raised when:

   - The association is configured and the admin state is enabled, but the SCTP transport is not in the ASP-UP protocol state for the M3UA plugin, or
   - The association is configured, but the SCTP transport is not in the APP-UP state for other plugins

   Note: It is normal to have an association alarm if the association is in the Blocked or Disabled administrative state.

   This alarm is cleared when:

   - The association received an ASP-UP-ACK from the far-end and the SCTP transport in the ASP-UP state for the M3UA plugin, or
   - The SCTP transport is an APP-UP state for other plugins, or
   - The association is disabled/deleted

   If an association's protocol state does not match the association's administrative state, the system will automatically attempt to recover the association if configured as Initiator and enabled. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed association (default: 10 seconds).

   Association administrative states are set from **Main Menu** > **Transport Manager** > **Maintenance** > **'Transport'** by clicking on the desired action for the row containing the association. This screen is also used to monitor association status.

To troubleshoot:

- If the association is manually Blocked or Disabled, then no further action is necessary.
- Verify that the association's local IP address and port number are configured on the IP signaling gateway (Some signaling gateways will only accept connections from IP addresses and ports that they are configured to accept from).
- Verify that the association's remote IP address and port correctly identify an SCTP listening port on the adjacent server.
- Verify that IP network connectivity exists between the MP server and the adjacent server.
- Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
- Verify that the adjacent server on the signaling gateway is not under maintenance.

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

19401 - Failed to configure Transport

Event Type: TMF

Description: Failed to configure Transport

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrFailedToConfigureTransportNotify

Recovery:

1. A Transport is configured each time the Transport attempts to connect or reconnect.
2. If transport configuration fails or the alarm persists, contact *My Oracle Support (MOS)* for assistance.

19402 - Failed to connect Transport

Event Type: TMF

Description: Failed to connect Transport

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 60

OID: awptransmgrFailedToConnectTransportNotify

Recovery:

1. The Transport named in the Instance field has failed in a connection attempt. If configured as an SCTP Initiator, the system will automatically attempt to recover the association/connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport

Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If configured as an SCTP or UDP Listener, no further action is taken.

To troubleshoot

- Verify that the transport's local IP address and port number are configured on the Adjacent Node (Some Nodes will only accept connections from IP addresses and ports they are configured to accept connections from).
- Verify that the transport's remote IP address and port correctly identify an SCTP listening port on the adjacent node.
- Verify that IP network connectivity exists between the MP and the adjacent node.
- Verify that the timers in the transport's configuration set are not set too short to allow the connection to proceed. This should be rare if the IP network is functioning correctly.
- Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
- Verify that the adjacent server on the signaling gateway is not under maintenance.

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

19403 - Received malformed SCTP message (invalid length)

Alarm Group: TMF

Description: Received malformed SCTP message (invalid length)

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrReceivedMalformedTransSctpMessageNotify

Recovery:

1. An SCTP message was received containing a message not valid in length.
2. If the alarm persists, contact *My Oracle Support (MOS)*.

19404 - Far-end closed the Transport

Event Type: TMF

Description: Far-end closed the Transport

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 10

OID: awptransmgrFarEndClosedTheTransportNotify

Recovery:

1. The far-end of the SCTP association sent a SHUTDOWN or ABORT message to close the association. If an Initiator, the MP server automatically attempts to reestablish the connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed association (default: 10 seconds). If a Listener, the MP server will only open the socket and await further messages from the far-end.

   To Troubleshoot:

   - Investigate the adjacent node at the specified IP address and port to determine if it failed or if it is under maintenance.
   - Check the adjacent node for alarms or logs that might indicate the cause for their closing the association.

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

19405 - Transport closed due to lack of response

Event Type: TMF

Description: Transport closed due to lack of response

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 10

OID: awptransmgrTransportClosedDueToLackOfResponseNotify

Recovery:

1. The adjacent node at the specified IP address and port failed to respond to attempts to deliver an SCTP DATA packet or SCTP heartbeat. If an SCTP Initiator, the transport is closed and the MP server automatically attempts to reestablish the connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If a Listener, the MP server will only open the socket and await further messages from the far-end.

   To troubleshoot:

   - Verify that IP network connectivity still exists between the MP server and the adjacent server.
   - Verify that the timers in the transport's configuration set are not set too short to allow the signaling to succeed. This should be rare if the IP network is fuctioning correctly.
   - Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
   - Verify that the adjacent server on the signaling gateway is not under maintenance.

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

19406 - Local Transport maintenance state change

Event Type: TMF

Description: Local Transport maintenance state change

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrLocalTransportMaintenanceStateChangeNotify

Recovery:

1. No customer action is necessary if this was an expected change due to some maintenance activity. Otherwise, security logs can be examined on the NO/SO server to determine which user changed the administrative state.

   Transport status can be viewed using **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.

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

19407 - Failed to send Transport DATA Message

Event Type: TMF

Description: Failed to send Transport DATA Message

Severity: Info

Instance: <TransportName>, <TransportAdapter>, <TransportProtocol>

HA Score: Normal

Throttle Seconds: 10

OID: awptransmgrFailedToSendTransDataMessageNotify

Recovery:

1. An attempt to send an SS7 M3UA/ENUM DATA message has failed. The message has been discarded.

   For SCTP, Possible reasons for the failure include:

   - The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing hte MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
   - The socket has closed just as the send was being processed.

   To Troubleshoot:

   - Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
   - Verify that the adjacent server on the signaling gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.

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

19408 - Single Transport Egress-Queue Utilization

Alarm Group: TMF

Description: The percent utilization of the MP's single Transport Egress-Queue is approaching its maximum capacity

Severity: Based on defined Thresholds. Minor, Major, Critical Engineered Max Value = 1000

Instance: <TransportName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: awptransmgrTransSingleWriteQueueUtilNotify

Recovery:

1. The percent utilization of the MP's Transport Writer Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization, all new egress messages from the Transport will be discarded.

   This alarm should not normally occur when no other congestion alarms are asserted. This may occur for a variety of reasons:

   1. An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being received form the network.
   2. The SCTP Association Writer process may be experiencing a problem preventing it from processing events from its event queue. The alarm log should be examined form **Main Menu** > **Alarms & Events**.
   3. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining Mps in the server site. MP server status can be monitored form **Main Menu** > **Status & Control** > **Server Status**.
   4. The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
   5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Main Menu** > **Status & Control** > **KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

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

19409 - Message Rejected by ACL Filtering

Event Type: TMF

Description: The message is rejected based on configured Access Control List for Transport

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrMessageRejectedByAclFilteringNotify

Recovery:

1. Verify that the ENUM Server's IP address is the ACL, or that the ACL is empty.
2. If the alarm persists, contact *My Oracle Support (MOS)*.

19410 - Adjacent Node IP Address state change

Event Type: TMF

Description: State change of an IP Address of a multihomed Adjacent Node in SCTP Transport

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrAdjIpAddrStateChangeNotify

Recovery:

1. Verify that IP network connectivity still exists between the MP server and the adjacent server.
2. If the alarm persists, contact *My Oracle Support (MOS)* .

19411 - SCTP Transport closed due to failure of multihoming validation

Event Type: TMF

Description: SCTP Transport closed due to failure of multihoming validation

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrSctpTransportRefusedNotify

Recovery:

1. Recheck the Adjacent Node's configure IP Address and validation mode.
2. If alarm persists, contact *My Oracle Support (MOS)* .

19412 - SCTP Transport Transport Configuration Mismatch

Event Type: TMF

Description: IP address advertised by an Adjacent Node in INIT/INIT-ACK chunk are different from configured IP Addresses

Severity: Info

Instance: <TransportName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrSctpTransportCfgMismatchNotify

Recovery:

1. Recheck the Configured IP Address and Transport configuration and validation mode.
2. If the alarm persists, contact *My Oracle Support (MOS)*.

19413 - SCTP Transport closed due to unsupported peer type evenet recieved.

Alarm Group: TMF

Description: SCCTP Transport closed due to unsupported add/delete peer IP Address event recieved in Peer Address Notification

Severity: Info

Instance: TransportName

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: awptransmgrTransportClosedDueToUnsupportedEventNotify

Recovery:

1. Disable SCTP Dynamic Address Reconfiguration at the Adjacent Node.
2. If the alarm persists, contact *My Oracle Support (MOS)*.

Communication Agent, ComAgent (19800-19909)

This section provides information and recovery procedures for Communication Agent (ComAgent) alarms and events, ranging from 19800 - 19909, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

19800 - Communication Agent Connection Down

Alarm Group: CAF

Description: This alarm indicates that a Communication Agent is unable to establish transport connections with one or more other servers, and this may indicate that applications on the local server are unable to communicate with all of their peers. Generally this alarm is asserted when a server or the IP network is undergoing maintenance or when a connection has been manually disabled.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnectionDownNotify

Recovery:

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

4. If the connection is manually disabled, then no further action is necessary.

5. Verify that the remote server is not under maintenance.

6. Verify that IP network connectivity exists between the two connection end-points.

7. Verify that the connection's local IP address and port number are configured on remote Node.

8. Verify that the Application Process using Communication Agent plug-in is running on both ends.

9. Verify that the connection's remote IP address and port correctly identify remote's listening port.

10. Contact *My Oracle Support (MOS)* for assistance.

19801 - Communication Agent Connection Locally Blocked

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnLocalBlockedNotify

Recovery:

This alarm is cleared when:

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

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

4. If the expected set of connections is locally blocked, then no further action is necessary.

5. To remove a the local block condition for a connection, use the **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screen and click the 'Enable' action button for the desired connection.

6. Contact *My Oracle Support (MOS)* for assistance.

19802 - Communication Agent Connection Remotely Blocked

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnRemoteBlockedNotify

Recovery:

This alarm is cleared when:

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

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

4. If the expected set of connections is locally blocked, then no further action is necessary.

5. To remove a the local block condition for a connection, use the **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screen and click the 'Enable' action button for the desired connection.

6. Contact *My Oracle Support (MOS)* for assistance.

19803 - Communication Agent stack event queue utilization

Alarm Group: CAF

Description: The percent utilization of the Communication Agent Task stack queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded, based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode.

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFQueueUtilNotify

Recovery:

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

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

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

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

    Contact *My Oracle Support (MOS)* for assistance.

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

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

    Contact *My Oracle Support (MOS)* for assistance.

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

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 300 (5 min)

OID: cAFClientConnWaitNotify

Recovery:

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

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

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

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

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. Verify that the remote server is not under maintenance.
5. If the connection is manually disabled at the client MP, and it is expected to be disabled, then no further action is necessary.
6. If the connection has been manually disabled at the client MP, but it is not supposed to be disabled, then enable the connection by clicking on the 'Enable' action button on the Connection Status screen.
7. Verify that IP network connectivity exists between the two connection end-points.

8. Verify that the connection's local IP address and port number are configured on remote client MP.

9. Verify that the Application Process using Communication Agent plug-in is running on both ends.

10. Verify that the connection's remote IP address and port correctly identify remote's listening port.

11. Contact *My Oracle Support (MOS)* for assistance.

19805 - Communication Agent Failed To Align Connection

Alarm Group: CAF

Description: The Communication Agent failed to align connection. This alarm indicates that Communication Agent has established one or more transport connections with servers that are running incompatible versions of software, and so Communication Agent is unable to complete the alignment of the connection. A connection that fails alignment cannot be used by applications to communicate with other servers, and so this alarm may indicate that applications are unable to communicate with their expected set of peers.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnAlignFailedNotify

Recovery:

1. If the connection administrative action is set to 'disable', the alarm is cleared. No further action is necessary.

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

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

4. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

5. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

   For each connection reporting 'Aligning' connection status, determine the servers that are endpoints, and verify that the correct software is installed on each server. If incorrect software is present, then server maintenance may be required.

6. Contact *My Oracle Support (MOS)* for assistance.

19806 - Communication Agent CommMessage mempool utilization

Alarm Group: CAF

Description: The percent utilization of the Communication Agent CommMessage mempool is approaching defined threshold capacity.

The percent utilization of the Communication Agent internal resource pool (CommMessage) is approaching its defined capacity. If this problem persists and the usage reaches 100% utilization, ComAgent will allocate the CommMessage objects from the heap. This should not impact the functionality, but may impact performance and/or latency.

Severity: Critical, Major, Minor

Instance: <ComAgent Process Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPoolResUtilNotify

Recovery:

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

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

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

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

   Contact *My Oracle Support (MOS)* for assistance.

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

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

   Contact *My Oracle Support (MOS)* for assistance.

19807 - Communication Agent User Data FIFO Queue utilization

Alarm Group: CAF

Description: The percent utilization of the Communication Agent User Data FIFO Queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded, based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode.

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFUserDataFIFOUtilNotify

Recovery:

1. An IP network or Adjacent node problem may exist preventing from transmitting messages into the network at the same pace that messages are being received from the network.
2. Use **Main Menu** > **Alarms & Events** to determine if the ComAgent worker thread may be experiencing a problem preventing it from processing events from User Data FIFO queue.

   Contact *My Oracle Support (MOS)* for assistance.

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

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

   Contact *My Oracle Support (MOS)* for assistance.

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

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

   Contact *My Oracle Support (MOS)* for assistance.

19808 - Communication Agent Connection FIFO Queue utilization

Alarm Group: CAF

Description: The percent utilization of the Communication Agent Connection FIFO Queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new ComAgent internal Connection Management StackEvents messages can be discarded based on Application's Global Congestion Threshold Enforcement Mode.

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFMxFIFOUtilNotify

Recovery:

1. An IP network or Adjacent node problem may exist preventing from transmitting messages into the network at the same pace that messages are being received from the network.
2. Use **Main Menu** > **Alarms & Events** to determine if the ComAgent worker thread may be experiencing a problem preventing it from processing events from ComAgent Connection FIFO queue.

   Contact *My Oracle Support (MOS)* for assistance.

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

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

Contact *My Oracle Support (MOS)* for assistance.

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

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

Contact *My Oracle Support (MOS)* for assistance.

19810 - Communication Agent Egress Message Discarded

Event Type: CAF

Description: Communication Agent Egress Message Discarded.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventEgressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

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

2. If it's a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.

3. If the event is raised due to software condition, It's an indication that the Communication Agent Process may be experiencing problems.

4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.

5. Contact *My Oracle Support (MOS)* for assistance.

19811 - Communication Agent Ingress Message Discarded

Event Type: CAF

Description: Communication Agent Ingress Message Discarded.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventIngressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

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

2. If it's a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.

3. If the event is raised due to software condition, it is an indication that the Communication Agent Process may be experiencing problems.

4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.

5. Contact *My Oracle Support (MOS)* for assistance.

19814 - Communication Agent Peer has not responded to heartbeat

Event Type: CAF

Description: Communication Agent Peer has not responded to heartbeat.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventHeartbeatMissedNotify

Recovery:

1. Check the configuration of managed objects and resolve any configuration issues with the Managed Object or hosting nodes.

   This message may be due to network condition or latency or due to setup issues.

2. If the event is raised due to software condition, It's an indication that the Communication Agent Process may be experiencing problems.

3. Use **Main Menu** > **Alarms & Events** and examine the alarm log.

4. Contact *My Oracle Support (MOS)* for assistance.

19816 - Communication Agent Connection State Changed

Event Type: CAF

Description: Communication Agent Connection State Changed.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventConnectionStateChangeNotify

Recovery:

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

   This Event is a log of connection state change.

2. Contact *My Oracle Support (MOS)* for assistance.

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

Event Type: CAF

Description: Communication Agent DB Responder detected a change in configurable control option parameter.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtConfigParamChangeNotify

Recovery:

This event is an indication that Communication Agent detected a control parameter change. The change will be applied to applicable software component. If the change is applied on the GUI, the appropriate GUI action is logged in security logs. If the action is not performed from GUI and the control parameter is changed, this event indicates the executed change.

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

19818 - Communication Agent DataEvent Mempool utilization

Event Type: CAF

Description: The percent utilization of the Communication Agent DataEvent Mempool is approaching defined threshold capacity.

Severity: Minor, Major, Critical

Instance: <ComAgent Process>

HA Score: Normal

Throttle Seconds: 86400

OID: cAFDataEvPoolResUtilNotify

Recovery:

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

19820 - Communication Agent Routed Service Unavailable

Alarm Group: CAF

Description: This alarm indicates that all connections of all connection groups associated with a Routed Service are unavailable. This generally occurs when far-end servers have been removed from service

by maintenance actions. This can also occur if all of the Routed Service's connections have been either disabled or blocked.

Severity: Major

Instance: <RoutedServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSUnavailNotify

Recovery:

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

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. Contact *My Oracle Support (MOS)* for assistance.

19821 - Communication Agent Routed Service Degraded

Alarm Group: CAF

Description: This alarm indicates that some, but not all, connections are unavailable in the connection group being used by a Communication Agent Routed Service to route messages. The result is that the server that posted this alarm is not load-balancing traffic across all of the connections configured in the connection group.

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSDegradedNotify

Recovery:

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

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. Contact *My Oracle Support (MOS)* for assistance.

19822 - Communication Agent Routed Service Congested

Alarm Group: CAF

Description: This alarm indicates that a routed service is load-balancing traffic across all connections in a connection group, but all of the connections are experiencing congestion. Messages may be discarded due to congestion.

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSCongestedNotify

Recovery:

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

   If the far-end servers are overloaded, then it is possible that the system is being presented a load that exceeds its engineered capacity. If this is the case, then either the load must be reduced, or additional capacity must be added.

4. Contact *My Oracle Support (MOS)* for assistance.

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

Alarm Group: CAF

Description: Communication Agent routed service is routing traffic using a connection group that has a lower-priority than another connection group.

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSUsingLowPriConnGrpNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the the reasons why connections are unavailable.

3. Use **Main Menu** > **Status & Manage** > **Server** to confirm that the far-end servers have an application state of enabled, and that their subsystems are operating normally.

It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. Contact *My Oracle Support (MOS)* for assistance.

19824 - Communication Agent Pending Transaction Utilization

Alarm Group: CAF

Description: The ComAgent Reliable Transfer Function is approaching or exceeding its engineered reliable transaction handling capacity.

Severity: Minor, Major, Critical

Instance: n/a (ComAgent process)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTransUtilNotify

Recovery:

1. Use **Main Menu** > **Status & Control** > **Server Status** to view MP server status.
2. Remote server is slow in responding to outstanding transaction with correlation resource in-use. The mis-configuration of ComAgent Server/Client routing may result in too much traffic being distributed to affected connection for MP.
3. There may be an insufficient number of Server Application MPs configured to handle the internal traffic load. If server application MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. Use **Main Menu** > **Alarm & Events** and examine the alarm log.

The system may be experiencing network problems.

The Communication Agent Process may be experiencing problems.

5. Contact *My Oracle Support (MOS)* for assistance.

19825 - Communication Agent Transaction Failure Rate

Alarm Group: CAF

Description: The number of failed transactions during the sampling period has exceeded configured thresholds.

Severity: Minor, Major, Critical

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTransFailRateNotify

Recovery:

1. Use **Main Menu** > **Status & Control** > **Server Status** to view MP server status.

2. Remote server is slow in responding to outstanding transaction with correlation resource in-use. The mis-configuration of ComAgent Server/Client routing may result in too much traffic being distributed to affected connection for MP.

3. There may be an insufficient number of Server Application MPs configured to handle the internal traffic load. If server application MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

4. Use **Main Menu** > **Alarm & Events** and examine the alarm log.

   The system may be experiencing network problems.

   The Communication Agent Process may be experiencing problems.

5. Contact *My Oracle Support (MOS)* for assistance.

19826 - Communication Agent Connection Congested

Alarm Group: CAF

Description: This alarm indicates that Communication Agent is experiencing congestion in communication between two servers, and this can be caused by a server becoming overloaded or by network problems between two servers.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnCongestedNotify

Recovery:

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

3. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

4. If the Remote MP Overload Level (OL) > 0 then determine why the remote server is congested.
   a) Verify that the remote server is not under maintenance.
   b) Examine the remote's CPU utilization.
   c) Examine the remote's current alarms.

5. If the local server's Transport Congestion Level (TCL) > 0 then determine why the connection is not handling the load.
   a) The remote may be overload by traffic from other MPs.
   b) The local server may be trying to send too much traffic to the remote.
   c) The IP connectivity may be impaired.

6. Contact *My Oracle Support (MOS)* for assistance.

19830 - Communication Agent Service Registration State Change

Event Type: CAF

Description: Communication Agent Service Registration State Change.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtSvcRegChangedNotify

Recovery:

This event is a log of normal application startup and shutdown activity. It may provide aid during trouble shooting when compared to other events in the log.

19831 - Communication Agent Service Operational State Changed

Event Type: CAF

Description: Communication Agent Service Operational State Changed.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtSvcOpStateChangedNotify

Recovery:

1. This event indicates that a Communication Agent service changed operational state, and typically results from maintenance actions.

   A service can also change state due to server overload.

2. If the state change is unexpected, then Contact *My Oracle Support (MOS)* for assistance.

19832 - Communication Agent Reliable Transaction Failed

Event Type: CAF

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

Severity: Info

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

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

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventComAgtTransFailedNotify

Recovery:

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

19833 - Communication Agent Service Egress Message Discarded

Event Type: CAF

Description: Communication Agent Service Egress Message Discarded.

Severity: Info

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

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

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventRoutingFailedNotify

Recovery:

1. View the Event AddlInfo column.

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

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

19842 - Communication Agent Resource-Provider Registered

Event Type: CAF

Description: Communication Agent Resource-Provider Registered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceProviderRegisteredNotify

Recovery:

No action required.

19843 - Communication Agent Resource-Provider Resource State Changed

Event Type: CAF

Description: Communication Agent Resource-Provider Resource State Changed.

Severity: Info

Instance: <ProviderServerName>: <ResourceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventResourceStateChangeNotify

Recovery:

No action required.

19844 - Communication Agent Resource-Provider Stale Status Received

Event Type: CAF

Description: Communication Agent Resource-Provider Stale Status Received.

Severity: Info

Instance: <ProviderServerName>: <ResourceName>

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventStaleHBPacketNotify

Recovery:

If this event is occurring frequently then check the ComAgent maintenance screens for other anomalies and to troubleshoot further.

19845 - Communication Agent Resource-Provider Deregistered

Event Type: CAF

Description: Communication Agent Resource-Provider Deregistered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceProviderDeRegisteredNotify

Recovery:

No action required.

19846 - Communication Agent Resource Degraded

Alarm Group: CAF

Description: Communication Agent Resource Degraded. A local application is using the resource, identified in the alarm, and the access to the resource is impaired. Some of the resource providers are either unavailable and/or congested.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFResourceCongestedNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which sub-resources are unavailable or degraded for the server that asserted the alarm.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if connections have failed or have congested.
3. Contact *My Oracle Support (MOS)* for assistance.

19847 - Communication Agent Resource Unavailable

Alarm Group: CAF

Description: Communication Agent Resource Unavailable. A local application needs to use a ComAgent resource, but the resource is unavailable. The resource can be unavailable if the local server has no ComAgent connections to servers providing the resource or no servers host active instances of the resource's sub-resources.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFResourceUnavailNotify

Recovery: Check the Communication Agent Connection Status maintenance screen

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to verify that the local server is connected to the expected servers.

   If the local server reports unavailable connections, then take actions to troubleshoot the cause of the connection failures.

2. If the ComAgent connections are InService, use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which servers are providing the resource.

   If no servers are providing the resource, then the most likely reason is that maintenance actions have been taken that have removed from service the application that provides the concerned resource.

3. Contact *My Oracle Support (MOS)* for assistance.

19848 - Communication Agent Resource Error

Alarm Group: CAF

Description: Communication Agent Resource Error. Two sets of servers are using incompatible configurations for a ComAgent resource.

Severity: Minor

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 50

OID: cAFResourceErrorNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which sets of servers are incompatible.

   Check the incompatible servers to verify that they are operating normally and are running the expected versions of software.

2. Contact *My Oracle Support (MOS)* for assistance.

19850 - Communication Agent Resource-User Registered

Event Type: CAF

Description: Communication Agent Resource-User Registered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceUserRegisteredNotify

Recovery:

No action required.

19851 - Communication Agent Resource-User Deregistered

Event Type: CAF

Description: Communication Agent Resource-User Deregistered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceUserDeRegisteredNotify

Recovery:

No action required.

19852 - Communication Agent Resource Routing State Changed

Event Type: CAF

Description: Communication Agent Resource Routing State Changed.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventResourceRoutingStateNotify

Recovery:

No action required.

19853 - Communication Agent Resource Egress Message Discarded

Event Type: CAF

Description: Communication Agent Resource Egress Message Discarded.

Severity: Info

Instance: <ResourceName>: <SubResourceID>

Note: If the resource is unknown, then <ResourceName> is the ResourceID converted to text. The <SubResourceID> is an integer converted to text, regardless of whether it is known or unknown.

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventHaEgressMessageDiscardedNotify

Recovery:

1. Message is being discarded due to one of the reasons specified in Event AddlInfo.

   If the condition is persistent with the status of one of the ComAgent Configuration Managed Objects there is an underlying issue with the Managed Object.

2. Use **Main Menu** > **Alarms & Events** and examine the alarm log for ComAgent Process problems.

3. Contact *My Oracle Support (MOS)* for assistance.

19854 - Communication Agent Resource-Provider Tracking Table Audit Results

Event Type: CAF

Description: Communication Agent Resource-Provider Tracking Table Audit Results. This event is generated when a Resource Provider Tracking Table (RPTT) entry with Status equal to Auditing is replaced with a new status (null, Active, Standby, Spare, OOS, etc) and there are no other RPTT entries, for this specific Resource/SR, with Status equal to Auditing.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventHaRPTTAuditResultNotify

Recovery:

   No action required.

19855 - Communication Agent Resource Has Multiple Actives

Alarm Group: CAF

Description: This alarm indicates a possible IP network disruption that has caused more than one Resource Provider to become Active. The server that asserted this alarm expects there to be only one active Resource Provider server for the Resource, but instead it is seeing more than one. During this condition the server may be sending commands to the wrong Resource Provider. This may affect applications such as CPA, PDRA.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFMultipleActivesNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which Resource Provider servers are announcing 'Active' status for the Resource.
2. Investigate possible IP network isolation between these Resource Provider servers.
3. Contact *My Oracle Support (MOS)* for assistance.

19856 - Communication Agent Service Provider Registration State Changed

Event Type: CAF

Description: The Communication Agent Service Provider Registration State has changed.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventSvcProvRegStateChangedNotify

Recovery:

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

19857 - Communication Agent Service Provider Operational State Changed

Event Type: CAF

Description: The Communication Agent Service Provider Operational State has Changed

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventSvcProvOpStateChangedNotify

Recovery:

1. This event indicates that a ComAgent service provider changed operational state, and typically results from maintenance actions. A service can also change state due to overload.
2. If the state change is unexpected, contact *My Oracle Support (MOS)*.

19858 - Communication Agent Connection Rejected

Event Type: CAF

Description: The Communication Agent receives a connection request from an unknown server.

Severity: Info

Instance: RemoteIp

HA Score: Normal

Throttle Seconds: 1800

OID: cAFEventSvcProvOpStateChangedNotify

Recovery:

1. Verify network routes are correctly configured for ComAgent.
2. If assistance is required, contact *My Oracle Support (MOS)*.

19860 - Communication Agent Configuration Daemon Table Monitoring Failure

Alarm Group: CAF

Description: This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTableMonitorFailureNotify

Recovery:

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.

3. If conditions do not permit a forced failover of the active NOAM, then contact *My Oracle Support (MOS)* for assistance.

4. If conditions permit, then initiate a failover of active NOAM.

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

5. After NOAM failover completes, verify that the alarm has cleared.

6. If the alarm has not cleared, then Contact *My Oracle Support (MOS)* for assistance.

19861 - Communication Agent Configuration Daemon Script Failure

Alarm Group: CAF

Description: This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFScriptFailureNotify

Recovery:

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this server.

3. If conditions do not permit a forced failover of the active NOAM, then contact *My Oracle Support (MOS)* for assistance.

4. If conditions permit, then initiate a failover of active NOAM.

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

5. After NOAM failover completes, verify that the alarm has cleared.

6. If the alarm has not cleared, then Contact *My Oracle Support (MOS)* for assistance.

19862 - Communication Agent Ingress Stack Event Rate

Alarm Group: CAF

Description: The Communication Agent Ingress Stack Event Rate is approaching its defined threshold capacity.

Severity:

- Minor - if exceeding 100K on Gen8 hardware, 75k on other hardware
- Major - if exceeding 110K on Gen8 hardware, 80k on other hardware
- Critical - if exceeding 120K on Gen8 hardware, 84k on other hardware

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFIngressRateNotify

Recovery:

1. This alarm indicates that a server is overrunning its defined processing capacity. If any of the defined threshold onset levels are exceeded, Communication Agent will discard comparatively low priority messages. Check the configuration, routing, and deployment mode capacity.

2. Contact *My Oracle Support (MOS)* for further assistance.

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group: CAF

Description: The maximum number of connections per connection group limit has been reached.

Severity: Info

Instance: <Connection group name>

HA Score: Normal

Throttle Seconds: 86400

OID: cAFComAgentMaxConnsInConnGrpNotify

Recovery:

1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.

2. Contact *My Oracle Support (MOS)* for further assistance.

19864 - ComAgent Successfully Set Host Server Hardware Profile

Event Group: CAF

Description: ComAgent successfully set the host server hardware profile.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventSuccessSetHostServerHWProfileNotify

Recovery:

1. This event indicates that all TPS controlling parameter values are successfully set for the host server hardware profile.

2. If needed, contact *My Oracle Support (MOS)*.

19865 - ComAgent Failed to Set Host Server Hardware Profile

Event Group: CAF

Description: ComAgent failed to set the host server hardware profile.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventFailToSetHostServerHWProfileNotify

Recovery:

1. This event indicates that there is a failure in applying default hardware settings for ComAgent TPS controlling parameters. When default settings also fail to apply, then the factory values will be used for the TPS controlling parameters.

2. If needed, contact *My Oracle Support (MOS)*.

19866 - Communication Agent Peer Group Status Changed

Event Type: CAF

Description: The Communication Agent Peer Group operational status has changed

Severity: Info

Instance: RemoteIp

HA Score: Normal

Throttle Seconds: N/A

OID: cAFEventPeerGroupStatusChangeNotify

Recovery:

Generally, this alarm is informational and no action is required.

19867 - Communication Agent Peer Group Egress Message Discarded

Event Type: CAF

Description: The Communication Agent Peer Group egress message is being discarded due to one of the following reasons:

- Unknown Peer Group
- Peer Group Unavailable
- Peer Congested
- Reliability not supported

Severity: Info

Instance: RemoteIp

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventPSEgressMessageDiscardedNotify

Recovery:

Generally, this alarm is informational and no action is required.

19900 - Process CPU Utilization

Alarm Group: STK

Description: The Process, which is responsible for handling all Signaling traffic, is approaching or exceeding its engineered traffic handling capacity.

Severity: Critical, Major, Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcProcessCpuUtilizationNotify

Recovery:

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

   - The mis-configuration of Server/Client routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
   - There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the traffic load to the server site is exceeding its capacity.

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

   Contact *My Oracle Support (MOS)* for assistance.

19901 - CFG-DB Validation Error

Alarm Group: STK

Description: A minor database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbValidationErrorNotify

Recovery:

An unexpected condition has occurred while performing a database update, but database updates are still enabled.

Contact *My Oracle Support (MOS)* for assistance.

19902 - CFG-DB Update Failure

Alarm Group: STK

Description: A critical database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are DISABLED.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbUpdateFailureNotify

Recovery:

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

Contact *My Oracle Support (MOS)* for assistance.

19903 - CFG-DB post-update Error

Alarm Group: STK

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbPostUpdateErrorNotify

Recovery:

An unexpected condition has occurred while performing a database update, but database updates are still enabled.

Contact *My Oracle Support (MOS)* for assistance.

19904 - CFG-DB post-update Failure

Alarm Group: STK

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

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbPostFailureNotify

Recovery:

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

Contact *My Oracle Support (MOS)* for assistance.

19905 - Measurement Initialization Failure

Alarm Group: STK

Description: A measurement object failed to initialize.

Severity: Critical

Instance: <measTagName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcMeasurementInitializationFailureNotify

Recovery:

Measurement subsystem initialization has failed for the specified measurement.

Contact *My Oracle Support (MOS)* for assistance.

Diameter Signaling Router (DSR) Diagnostics (19910-19999)

This section provides information and recovery procedures for DSR alarms and events, ranging from 19910-19999, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

19910 - Message Discarded at Test Connection

Event Type: DIAG

Description: Normal traffic is being discarded because it is routed to an egress Test Connection. An egress Test Connection is given a normal message to be transmitted.

Severity: Major

Instance: <Connection name>

HA Score: Normal

Throttle Seconds: 86400

OID: dbcNormalMessageDiscardedNotify

Recovery:

1. Update routing rules to exclude Test connections from being used for routing.

   Normal traffic should be received and sent on non-test connections.

2. Change the hostname of the peer connected to the test connection.

   The hostname of the peer connected to the test connection may be the destination host for the incoming normal traffic.

19911 - Test message discarded

Event Type: DIAG

Description: Test message is given to a non-test connection to be transmitted.

Severity: Info

Instance: <Connection name>

HA Score: Normal

Throttle Seconds: 5

OID: dbcDiagnosticMessageDiscardNotify

Recovery:

Update routing rules to exclude Test messages from being routed to non-test connection.

Test messages should be received and sent only on test connections.

Diameter Alarms and Events (22000-22350, 22900-22999)

22001 - Message Decoding Failure

Event Type: DIAM

Description: A message received from a peer was rejected because of a decoding failure. Decoding failures can include missing mandatory parameters. A Diameter message was received either without the mandatory Destination-Realm AVP or, while parsing the message, the message content was inconsistent with the Message Length in the message header.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterIngressMsgRejectedDecodingFailureNotify

Recovery:

These protocol violations are caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node (identified by the Peer Name) and cannot be fixed using the application.

22002 - Peer Routing Rules with Same Priority

Event Type: DIAM

Description: A peer routing table search with a received Request message found more than one highest priority Peer Routing Rule match. The system selected the first rule found but it is not guaranteed that the same rule will be selected in the future. It is recommended that Peer Routing Rules be unique for the same type of messages to avoid non-deterministic routing results.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterPeerRoutingTableRulesSamePriorityNotify

Recovery:

Modify one of the Peer Routing Rule Priorities using the **Diameter > Configuration > Peer Routing Rules** GUI page.

22003 - Application ID Mismatch with Peer

Event Type: DIAM

Description: While attempting to route a request message to a peer, a peer's transport connection was bypassed because the peer did not support the Application ID for that transport connection.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterApplicationIdMismatchWithPeerNotify

Recovery:

1. The system's peer routing table may be using a Route List containing a peer which does not support the Application ID or the list of Application IDs supported by the peer on each connection may

not be the same. The list of Application IDs that the peer supports on each connection can be viewed as follows:

a) Navigate to the GUI page: **Diameter > Maintenance > Connections**

b) Locate the relevant Peer Node and check the supported Application IDs.

2. If Application IDs are not the same for each connection (but should be) the Application ID for any connection can be refreshed by:

a) Navigate to the GUI page: **Diameter > Maintenance > Connections**

b) Locate the relevant **Connection**

c) Disable the **Connection**

d) Enable the **Connection**

3. The Diameter Node which originated the message (identified by the Origin-Host AVP) could be configured incorrectly and the application is trying to address a node which doesn't support the Application ID. This cannot be fixed using this application.

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

22004 - Maximum pending transactions allowed exceeded

Event Type: DIAM

Description: Routing attempted to select an egress transport connection to forward a message but the maximum number of allowed pending transactions queued on the connection has been reached.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterMaxPendingTxnsPerConnExceededNotify

Recovery:

The maximum number of pending transactions for each connection is set to a system-wide default value. If this event is occurring frequently enough for a particular connection then the maximum value may need to be increased. Contact *My Oracle Support (MOS)* for assistance.

22005 - No peer routing rule found

Event Type: DIAM

Description: A message not addressed to a peer (either Destination-Host AVP was absent or Destination-Host AVP was present but was not a peer's FQDN) could not be routed because no Peer Routing Rules matched the message.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterNoPrtRuleNotify

Recovery:

1. Either the message was incorrectly routed to this node or additional Peer Routing Rules need to be added. Existing Peer Routing Rules can be viewed and updated using **Diameter > Configuration > Peer Routing Rules** page.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22006 - Forwarding Loop Detected

Event Type: DIAM

Description: The Ingress Request message received was previously processed by the local node as determined from the Route-Record AVPs received in the message.

Severity: Info

Instance: <PeerName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterForwardingLoopDetectedNotify

Recovery:

1. An ingress Request message was rejected because message looping was detected. In general, the forwarding node should not send a message to a peer which has already processed the message (it should examine the Route-Record AVPs prior to message forwarding). If this type of error is occurring frequently, then the forwarding node is most likely incorrectly routing the message and the issue cannot be fixed using this application.
2. If Path Topology Hiding is activated and Protected Network Node's Route-Records are obscured with PseudoNodeFQDN, then inter-network ingress message loop detection could reject the message if same Request message is routed back to DEA. If this type of error is occurring, then the forwarding node is most likely mis-routing the message back to DEA.
3. If the problem persists, contact *My Oracle Support (MOS)*.

22007 - Inconsistent Application ID Lists from a Peer

Event Type: DIAM

Description: The list of Application IDs supported by a peer during the Diameter Capabilities Exchange procedure on a particular transport connection is not identical to one of the list of Application IDs received from the peer over a different available transport connection to that peer.

Severity: Info

Instance: <PeerName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSupportedAppIdsInconsistentNotify

Recovery:

1. A peer with multiple transport connections has established a connection and provided a list of supported Application IDs which does match a previously established connection. This could prevent Request messages from being routed uniformly over the peer's transport connections because the decision to route a message containing an Application ID is based upon the list of Application IDs supported on each transport connection. The list of Application IDs that the peer supports on each connection can be viewed as follows:

   a) Navigate to **Diameter > Maintenance > Connections**.
   b) Locate the relevant Peer Node and check the supported Application IDs.

2. If Application IDs are not the same for each connection (but should be) the Application ID for any connection can be refreshed by:

   a) Navigate to **Diameter > Maintenance > Connections**.
   b) Locate the relevant Connection.
   c) Disable the Connection.
   d) Enable the Connection.

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

22008 - Orphan Answer Response Received

Event Type: DIAM

Description: An Answer response was received for which no pending request transaction existed, resulting in the Answer message being discarded. When a Request message is forwarded the system saves a pending transaction, which contains the routing information for the Answer response. The pending transaction is abandoned if an Answer response is not received in a timely fashion.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterOrphanAnswerResponseReceivedNotify

Recovery:

If this event is occurring frequently, the transaction timers may be set too low. The timer values can be viewed and/or modified using the **Diameter > Configuration > System Options** page.

22009 - Application Routing Rules with Same Priority

Event Type: DIAM

Description: An application routing table search with a received Request message found more than one highest priority application routing rule match. At least two application routing rules with the same priority matched an ingress Request message. The system selected the first application routing rule found.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterApplicationRoutingTableRulesSamePriorityNotify

Recovery:

1. It is recommended that application routing rules be unique for the same type of messages to avoid unexpected routing results. Peer routing rule priorities can be modified using **Diameter > Configuration > Application Routing Rules** page.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22010 - Specified DAS Route List not provisioned

Event Type: DIAM

Description: The DAS Route List specified by the message copy trigger point is not provisioned.

Severity: Info

Instance: <RouteListId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSpecifiedDasRouteListNotProvisionedNotify

Recovery:

1. Provisioning is incorrect/misconfigured. Verify provisioning and provision/correct provisioning.
2. If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22012 - Specified MCCS not provisioned

Event Type: DIAM

Description: The Message copy CfgSet attached to the original message by the trigger point is not provisioned

Severity: Info

Instance: <MCCS>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSpecifiedMCCSNotProvisionedNotify

Recovery:

1. Verify the configured value of MCCS with the trigger point.
2. Verify the Message Copy CfgSet (MCCS) provisioning is properly configured.
3. If the problem persists, contact *My Oracle Support (MOS)*.

22013 - DAS Peer Number of Retransmits Exceeded for Copy

Event Type: DIAM

Description: The configured number of Message Copy retransmits has been exceeded for the DAS Peer.

Severity: Info

Instance: <MCCS>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterNumberOfRetransmitsExceededToDasNotify

Recovery:

1. Verify the configured value of 'Max Retransmission Attempts'
2. Verify local provisioning to connections to intended DAS peer server(s) are in service and no network issues in path(s) to intended DAS peer server(s) exist.
3. Verify DAS peer provisioning to insure proper configuration.
4. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

22014 - No DAS Route List specified

Alarm Group: DIAM

Description: No valid DAS Route List was specified in the Message Copy Config Set.

Severity: Info

Instance: <RouteListId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterNoDasRouteListSpecifiedNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22015 - Connection Operational Status Inconsistency May Exist

Event Type: DIAM

Description: DSR was unable to update the Operational Status and Operation Reason attributes for a transport connection on the OAM.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterOperationalStatusInconsistencyNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Connections** to view the Operational Status and Operation Reason attributes for a Connection.

   The Operational Status and Operation Reason attributes for a Connection on the OAM may be temporarily out of date with the values on DSR.

   This occurs when an internal event queue size has been exceeded. This should rarely occur and the inconsistency should be cleared when the Connection's "Remote Busy State" changes again.

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

22016 - Peer Node Alarm Aggregation Threshold

Alarm Group: DIAM

Description: This alarm occurs when there are a 'Critical' number of Peer Node alarms for a single Network Element.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPeerNodeUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Peer Nodes** to monitor Peer status.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peer is not under maintenance.
5. Contact *My Oracle Support (MOS)* for assistance.

22017 - Route List Alarm Aggregation Threshold

Alarm Group: DIAM

Description: This alarm occurs when there are a 'Critical' number of Route List alarms for the Network Element.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Route Lists** to monitor Route List status.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List are not under maintenance.
5. Contact *My Oracle Support (MOS)* for assistance.

22018 - Maintenance Leader HA Notification to go Active

Alarm Group: DIAM

Description: This alarm occurs when a DA-MP has received a notification from HA that the Maintenance Leader resource should transition to the Active role.

Severity: Info

Instance: <MP Node ID>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterDaMpLeaderGoActiveNotificationNotify

Recovery:

No action necessary.

22019 - Maintenance Leader HA Notification to go OOS

Alarm Group: DIAM

Description: This alarm occurs when a DA-MP has received a notification from HA that the Maintenance Leader resource should transition to the OOS role.

Instance: <MP Node ID>

Severity: Info

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterDaMpLeaderGoOOSNotificationNotify

Recovery:

No action necessary.

22020 - Copy Message size exceeded the system limit

Event Type: DIAM

Description: The size of the message being copied to the DAS exceeded the maximum message size set system wide.

Severity: Info

Instance: <DA-MP>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterCopyMessageSizeExceededNotify

Recovery:

1. Verify the size of the Request and Answer messages and see it exceeds the system set message size.

   Use **Main** > **Diameter** > **Configuration** > **Route Lists** to correct provisioning.

2. Review provisioning and correct provisioning and see whether answers also needed to copy.

   Requests and answers may be copied to DAS.

3. If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22021 - Debug Routing Info AVP Enabled

Event Type: DIAM

Description: Debug Routing Info AVP is enabled.

Severity: Minor

Instance: None

HA Score: Normal

Throttle Seconds: 86400

OID: eagleXgDiameterDebugRoutingInfoAvpEnabledNotify

Recovery:

1. Change the IncludeRoutingInfoAvp parameter to *no* in the DpiOption table on the NO for a 2-tier system or on the SO for a 3-tier system.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22051 - Peer Unavailable

Alarm Group: DIAM

Description: Unable to access the Diameter Peer because all of the transport connections are Down.

Severity: Critical

Instance: <PeerName> (of the Peer which failed)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPeerUnavailableNotify

Recovery:

1. Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peer is not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22052 - Peer Degraded

Alarm Group: DIAM

Description: The peer has some available connections, but less than its minimum connection capacity. Continued routing to this peer may cause congestion or other overload conditions.

Severity: Major

Instance: <PeerName> (of the Peer which is degraded)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPeerDegradedNotify

Recovery:

1. Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peer is not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22053 - Route List Unavailable

Alarm Group: DIAM

Description: The Route List is Unavailable. A Route List becomes Unavailable when all of its peers become Unavailable and a Peer becomes Unavailable when all of its transport connections become Unavailable.

If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.

Severity: Critical

Instance: <RouteListName> (of the Route List which failed)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListUnavailableNotify

Recovery:

1. Route List status can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22054 - Route List Degraded

Alarm Group: DIAM

Description: The Route List's Operational Status has changed to Degraded because the capacity of the Route List's Active Route Group has dropped below the Route List's configured minimum capacity. There are two potential causes:

1. One or more of the Route List's peers become Unavailable. A Peer becomes Unavailable when all of its transport connections become Unavailable. If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.
2. The Route Groups within the Route List may not have been configured with sufficient capacity to meet the Route List's configured minimum capacity.

Severity: Major

Instance: <RouteListName> (of the Route List which is degraded)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListDegradedNotify

Recovery:

1. Route List status and configured minimum capacity can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22055 - Non-Preferred Route Group in Use

Alarm Group: DIAM

Description: The application has started to utilize a Route Group other than the highest priority Route Group to route Request messages for a Route List because the highest priority Route Group specified for that Route List has either become Unavailable or its capacity has dropped below the minimum capacity configured for the Route List while a lower priority Route Group has more capacity.

The preferred Route Group (i.e., with highest priority) is demoted from the Active Route Group to a Standby Route Group when a peer failure occurs causing the Route Group's Operational Status to change to Unavailable or Degraded. A Route Group becomes Degraded when its capacity has dropped below Route List's configured minimum capacity. A Route Group becomes Unavailable when all of its peers have an Operational Status of Unavailable or Degraded.

A Peer becomes Unavailable when all of its transport connections become Unavailable. If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.

Severity: Minor

Instance: <RouteListName> (of the concerned Route List)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterNonPreferredRouteGroupInUseNotify

Recovery:

1. Route List status and configured minimum capacity can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22056 - Connection Admin State Inconsistency Exists

Alarm Group: DIAM

Description: An operator request to change the Admin State of a transport connection was not completely processed due to an internal error. The admin state is either disabled from an egress routing perspective but the connection could not be taken out of service or the admin state is enabled from an egress routing perspective but the connection is not in service.

Severity: Major

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnAdminStateInconsistencyNotify

Recovery:

1. If the transport connection's Admin State is Disabled but the transport connection was not taken out of service due to an internal error do the following actions to correct the failure:
   a) Enable the connection via the following GUI menu: **Diameter** > **Maintenance** > **Connections**
   b) Wait for this alarm to clear.
   c) Disable the connection via the following GUI menu: **Diameter** > **Maintenance** > **Connections**

2. If the transport connection's Admin State is Enabled but the transport connection was not taken out of service due to an internal error do the following actions to correct the failure:
   a) Disable the connection via the following **Diameter** > **Maintenance** > **Connections**
   b) Wait for this alarm to clear.
   c) Enable the connection via the following GUI menu: **Diameter** > **Maintenance** > **Connections**

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

22057 - ETG Rate Limit Degraded

Alarm Group: DIAM

Description: The ETG Rate Limit has exceeded the defined threshold

Severity: Major

Instance: <ETGName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgRateLimitDegradedNotify

Recovery:

1. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Main Menu** > **Diameter** > **Maintenance** > **Connections** to determine if the sending Peers/Connections are offering too much traffic.
3. If the problem persists, contact *My Oracle Support (MOS)*.

22058 - ETG Pending Transaction Limit Degraded

Alarm Group: DIAM

Description: The ETG Pending Transactions Limit has exceeded the defined threshold

Severity: Major

Instance: <ETGName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgPendingTransLimitDegradedNotify

Recovery:

1. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.

2. Check the Egress Message Rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Main Menu** > **Diameter** > **Maintenance** > **Connections** to determine if the sending Peers/Connections are offering too much traffic.

3. Determine if the receiving Peers or Connections in the ETG are not responding with Answers in a timely manner because they are either busy or overloaded.

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

22059 - Egress Throttle Group Message Rate Congestion Level changed

Event Group: DIAM

Description: The Egress Throttle Group Message rate Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity: N/A

Instance: <ETGName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterEtgRateCongestionNotify

Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups**

2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and/or **Main Menu** > **Diameter** > **Maintenance** > **Connections**

3. Typically all routes to a server should be in an ETG. However, if that is not the case, alternate routes may be out of service and could cause overloading of traffic towards connections contained in this ETG. Evaluate traffic distribution to Server connections and see if any alternate routes to Server are unavailable causing overloading of traffic on an ETG.

4. Contact *My Oracle Support (MOS)* for assistance.

22060 - Egress Throttle Group Pending Transaction Limit Congestion Level changed

Event Group: DIAM

Description: The Egress Throttle Group Pending Transaction Limit Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity: N/A

Instance: <ETGName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterEtgPendingTransCongestionNotify

Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups**

2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and/or **Main Menu** > **Diameter** > **Maintenance** > **Connections**

3. Typically all routes to a server should be in a ETG, however if that is not the case, then those routes becoming out of service could cause overloading of traffic towards connections contained in this ETG. Evaluate traffic distribution to Server connections and see if any alternate routes to Server are unavailable causing overloading of traffic on an ETG.

4. The receiving Peers or Connections in the ETG are not responding with Answers in a timely manner. Check to see if they are busy or overloaded.

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

22061 - Egress Throttle Group Monitoring stopped

Alarm Group: DIAM

Description: ETG Rate and Pending Transaction Monitoring is stopped on all configured ETGs

Severity: Minor

Instance: <DA-MP Hostname>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgMonitoringStoppedNotify

Recovery:

1. Verify that ComAgent links setup between DA-MPs have not gone OOS causing SMS Service to not receive Responses from DA-MP Leader under **Main Menu** > **Communication Agent** > **Maintenance**.

2. Verify that ComAgent links are established between DA-MPs under **Main Menu** > **Communication Agent** > **Maintenance**

3. Verify the No-MP Leader condition in **Main Menu** > **Diameter** > **Maintenance** > **DA-MPs** > **Peer DA-MP Status** that at least 1 DA-MP is MP-Leader.

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

22062 - Actual Host Name cannot be determined for Topology Hiding

Event Type: Diameter

Description: Topology Hiding could not be applied because the Actual Host Name could not be determined

Severity: N/A

Instance: <CfgSetName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterTopoHidingActualHostNameNotFoundNotify

Recovery:

1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set.

2. If any DSR Applications are activated on DSR, ensure that any specific Application Level Topology Hiding feature is not conflicting with the contents of Actual Host Names specified in the MME Configuration Set.

3. Check if the first instance of a Session-ID AVP in the Request/Answer message contains the mandatory delimited ";".

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

22063 - Diameter Max Message Size Limit Exceeded

Event Type: DIAM

Description: The size of the message encoded by DSR has exceeded its max limits

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDiameterMaxMsgSizeLimitExceededNotify

Recovery:

No action required. However, if this event is seen to be incrementing consistently, contact *My Oracle Support (MOS)* for assistance.

22101 - Connection Unavailable

Alarm Group: DIAM

Description: Connection is unavailable for Diameter Request/Answer exchange with peer.

Note: This alarm is not added when the "Suppress Connection Unavailable Alarm" for a Transport Connection is set to "Yes".

Severity: Major

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnectionUnavailableAlarmNotify

Recovery:

1. Identify the most recent Connection Unavailable event in the event log for the connection and use the Event's recovery steps to resolve the issue.

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

22102 - Connection Degraded

Alarm Group: DIAM

Description: Connection is only available for routing messages with a priority greater than or equal to the connection's congestion level.

Severity: Major

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnectionDegradedAlarmNotify

Recovery:

1. Identify the most recent Connection Degraded event in the event log for the connection and use the Event's recovery steps to resolve the issue.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22103 - SCTP Connection Impaired

Alarm Group: DIAM

Description: One or more paths of the SCTP connection went down.

Severity: Minor

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterSCTPConnectionImpairedAlarmNotify

Recovery:

1. Identify the most recent SCTP Connection Impaired event in the event log for the connection and use the Event's recovery steps to resolve the issue.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22104 - SCTP peer is operating with a reduced IP address set

Alarm Group: DIAM

Description: The SCTP peer advertised less IP addresses than desired by the connection configuration. If two IP addresses have been configured for the Local Node of a certain SCTP connection, but following the SCTP connection establishment the peer node has advertised only one IP address (basically less than the number of IP addresses configured for the local node).

Severity: Minor

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterSCTPPeerReducedIPSetAlarmNotify

Recovery:

1. The peer is not able to advertise more than one IP address either due to an error in its configuration or due to being affected by a network interface failure. Check the networking configuration on the peer node.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22105 - Connection Transmit Congestion

Alarm Group: DIAM

Description: The connection transmit buffer is congested, messages will be discarded until this condition clears up. This error indicates that the socket write cannot complete without blocking, signaling that the socket buffer is currently full.

Severity: Major

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnectionTxCongestionAlarmNotify

Recovery:

1. The peer is not able to process the volume of traffic being offered on the connection. The traffic volume must be reduced, or processing capacity on the peer must be increased.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22106 - Ingress Message Discarded: DA-MP Ingress Message Rate Control

Alarm Group: DIAM

Description: An ingress message is discarded due to connection (or DA-MP) ingress message rate exceeding connection (or DA-MP) maximum ingress MPS.

Severity: Major

Instance: <MPHostName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIngressMessageDiscardedAlarmNotify

Recovery:

1. The ingress MPS on the DA-MP is exceeding the MP Maximum Ingress MPS. Consider decreasing the overall ingress message rate on the DA-MP by diverting the traffic or reducing the traffic.

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

22150 - FSM Anonymous Failure

Event Type: DIAM

Description: The anonymous connection has encountered a failure condition.

Severity: Info

Instance: <MpName>/<FailureCode>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterMpEvFsmAnonFailureNotify

Recovery:

No action required.

22170 - FSM Initiator Failure

Event Type: DIAM

Description: The initiator connection has encountered a failure condition.

Severity: Info

Instance: <TransConnName>/<FailureCode>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterEvFsmInitFailureNotify

Recovery:

No action required.

22200 - Local MP Congestion

Alarm Group: DIAM

Description: The Diameter Process is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterLocalMpCongestionNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of DIAMETER peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22201 - Ingress Message Rate

Alarm Group: DIAM

Description: The ingress message rate for the MP is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIngressMsgRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If the problem persists, contact *My Oracle Support (MOS)*.

22202 - PDU Buffer Pool Utilization

Alarm Group: DIAM

Description: The MP's PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPduBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22203 - PTR Buffer Pool Utilization

Alarm Group: DIAM

Description: The MP's PTR buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPtrBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page.

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

3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

4. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined from the **Alarms & Events** page.

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

22204 - Request Message Queue Utilization

Alarm Group: DIAM

Description: The MP's Request Message Queue Utilization is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress Request messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRequestMessageQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

4. If no additional congestion alarms are asserted, the Request Task may be experiencing a problem preventing it from processing messages from its Request Message Queue. The alarm log should be examined from the **Alarms & Events** page.

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

22205 - Answer Message Queue Utilization

Alarm Group: DIAM

Description: The MP's Answer Message Queue Utilization is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress Answer messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterAnswerMessageQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

4. If no additional congestion alarms are asserted, the Answer Task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. The alarm log should be examined from the **Alarms & Events** page.

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

22206 - Reroute Queue Utilization

Alarm Group: DIAM

Description: The MP's Reroute Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization any transactions requiring rerouting will be rejected. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRerouteQueueUtilNotify

Recovery:

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer time-outs. The status of connections should be examined from the **Diameter** > **Maintenance** > **Connections** page.

2. If no additional congestion alarms are asserted, the Reroute Task may be experiencing a problem preventing it from processing messages from its Reroute Queue. The alarm log should be examined using the **Alarms & Events** page.

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

22207 - All-Connections Event Queue Utilization

Alarm Group: DIAM

Description: The MP's All-Connections Event Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress transactions will be rejected. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterAllConnEventQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the task may be experiencing a problem preventing it from processing events from its All-Connections Event Queue. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22208 - Per-Connection Egress Message Queue Utilization

Alarm Group: DIAM

Description: The MP's per-connection egress message queue is approaching its maximum capacity.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPerConnMessageQueueUtilNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22209 - Message Copy Disabled

Alarm Group: DIAM

Description: Diameter Message Copy is disabled.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMessageCopyDisabledNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22214 - Message Copy Queue Utilization

Alarm Group: DIAM

Description: The MP's Message Copy queue utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMsgCopyQueueUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page.

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

3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

4. The Diameter Process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.

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

22215 - Ingress Message Discarded: DA-MP Overload Control

Alarm Group: DIAM

Description: Ingress message is discarded due to DA-MP CPU congestion

Severity: Major

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIngressMessageDiscardedOverLoadControlAlarmNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.

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

22216 - Ingress Message Discarded: Priority 0 message discarded by DA-MP Overload Control

Alarm Group: DIAM

Description: Ingress Priority 0 message discarded due to DA-MP CPU congestion.

Severity: Info

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressPri0MessageDiscardedNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22217 - Ingress Message Discarded: Priority 1 message discarded by DA-MP Overload Control

Alarm Group: DIAM

Description: Ingress Priority 1 message discarded due to DA-MP CPU congestion.

Severity: Info

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressPri1MessageDiscardedNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22218 - Ingress Message Discarded: Priority 2 message discarded by DA-MP Overload Control

Alarm Group: DIAM

Description: Ingress Priority 2 message discarded due to DA-MP CPU congestion.

Severity: Info

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressPri2MessageDiscardedNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22220 - Connection Congestion Level change

Event Type: DIAM

Description: The egress congestion level associated with the connection has changed. When a connection's egress queue is congested, the connection's operational status will be Degraded. If this problem persists and the queue reaches 100% utilization all new egress messages for the Connection will be discarded. This event should not normally occur when no other congestion alarms are asserted.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterConnCongestionLevelChangeNotify

Recovery:

1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.

2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.

3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.

4. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.

5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

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

22221 - Routing MPS Rate

Alarm Group: DIAM

Description: Message processing rate for this MP is approaching or exceeding its engineered traffic handling capacity. The routing mps rate (MPS/second) is approaching or exceeding its engineered traffic handling capacity for the MP.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRoutingMpsRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site.

   MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP.

   The routing mps rate of each MP can be monitored from **Main Menu** > **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load.

   The routing mps rate of each MP can be monitored from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state then the ingress message rate to the MP is exceeding its capacity to process the messages.

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

22222 - Long Timeout PTR Buffer Pool Utilization

Alarm Group: DIAM

Description: The MP's Long Timeout PTR buffer pool is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterLongTimeoutPtrBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**.

2. The misconfiguration of Pending Answer Timer assignment may result in excessive traffic being assigned to the Long Timeout PTR buffer Pool. View the Pending Answer Timer values via **Diameter** > **Configuration** > **Pending Answer Timers**. Examine the Pending Answer Timers assignment via the **Diameter** > **Configuration** > **Application Ids and Diameter** > **Configuration** > **Peer Nodes**.

3. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second

4. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

5. A software defect may exist resulting in Long Timeout PTR buffers not being de-allocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log from **Main Menu** > **Alarms & Events**.

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

22223 - DA-MP Memory Utilization Exceeded

Alarm Group: DIAM

Description: DA-MP memory utilization has exceeded its configured limits.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDaMpMemUtilizationExceededNotify

Recovery:

1. MPS exceeding its configured limits. Alarm *22221 - Routing MPS Rate* will be raised; perform the Recovery steps for this alarm.
2. Average hold time exceeding its configured limits. Alarm *22224 - Average Hold Time Limit Exceeded* will be raised. Perform the Recovery steps for this alarm.
3. Average message size exceeding its configured limits. Alarm *22225 - Average Message Size Limit Exceeded* will be raised. Perform the Recovery steps for this alarm.
4. Other. If the DA-MP is not exceeding any of the limits specified above, contact Oracle for assistance.

22224 - Average Hold Time Limit Exceeded

Alarm Group: DIAM

Description: The average transaction hold time has exceeded its configured limits.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterAvgHoldTimeLimitExceededNotify

Recovery:

The average transaction hold time is exceeding its configured limits, resulting in an abnormally large number of outstanding transactions. Reduce the average hold time by examining the configured Pending Answer Timer values and reducing any values that are unnecessarily large.

22225 - Average Message Size Limit Exceeded

Alarm Group: DIAM

Description: The size of the average message processed by DSR has exceeded its configured limits.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterAvgMsgSizeLimitExceededNotify

Recovery:

The size of the average message processed by DSR is exceeding its configured limits. This may cause DSR to consume an abnormally large amount of memory, leading to performance degradation. Alarm *22223 - DA-MP Memory Utilization Exceeded* may be raised as a result. Examine the traffic coming from connected peers to see if any of them are sending abnormally large messages.

22300 - Connection Unavailable: Socket configuration failure

Event Type: DIAM

Description: Software failure attempting to configure SCTP or TCP socket.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterConnUnavailSocketCfgFailureNotify

Recovery:

   Contact *My Oracle Support (MOS)*.

22301 - Connection Unavailable: Connection initiation failure

Event Type: DIAM

Description: Failure occurred while attempting to initiate SCTP or TCP connection with the peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterConnUnavailConnInitFailureNotify

Recovery:

1. Confirm that connection is not administratively Disabled at the peer.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches local connection configuration.
3. Confirm IP network connectivity between peer IP and local IP for the connection.
4. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22302 - Connection Unavailable: Received malformed message

Event Type: DIAM

Description: Diameter message received from peer with invalid or inconsistent header/AVP length fields.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedMalformedMessageNotify

Recovery:

1. Determine if other nodes/MPs connected to the peer are also experiencing problems with messages received from the peer. If so, the peer should be diagnosed.

2. Determine if other connections on this same MP are also experiencing problems. If so, the MP should be removed moved from service, replaced, and the *My Oracle Support (MOS)* should be contacted to assist with resolution.

22303 - Connection Unavailable: Peer closed connection

Event Type: DIAM

Description: The SCTP or TCP connection was closed by the peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailPeerClosedConnNotify

Recovery:

1. If unexpected, use peer node diagnostic/log information to determine why peer closed connection.

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

22304 - Connection Unavailable: Proving Failure

Event Type: DIAM

Description: Connection closed after DWR/DWA based proving algorithm failure.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailProvingFailureNotify

Recovery:

1. Examine the peer to determine why it is not responding to DWRs.

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

22305 - Connection Admin State change

Event Type: DIAM

Description: The Administrative state of the connection has changed.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnectionAdminStateChangeNotify

Recovery:

No action required.

22306 - Connection Unavailable: Timeout waiting for CER/CEA

Event Type: DIAM

Description: Connection closed after Tcex timer expired while waiting on CER or CEA from peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailTimedOutWaitingForCexNotify

Recovery:

1. For peer initiated connections, confirm that the configured Tcex timer value is not configured to be less than the expected time for peer to send CER after successfully initiating connection.
2. For locally initiated connections, confirm that the configured Tcex timer value is not less than the time expected for the peer to respond with CEA after receiving CER.
3. If the problem persists, contact *My Oracle Support (MOS)*.

22307 - Connection Unavailable: Timeout waiting for DPA

Event Type: DIAM

Description: Connection closed after Tdpa timer expired while waiting on DPA from peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailTimedOutWaitingForDpxNotify

Recovery:

No action required.

22308 - Received Unexpected CER/CEA

Event Type: DIAM

Description: CER or CEA message was received from the peer when it was not expected.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedUnexpectedCexNotify

Recovery:

1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact *My Oracle Support (MOS).*

22309 - Received Unexpected DWR/DWA

Event Type: DIAM

Description: DWR or DWA message was received from the peer when it was not expected.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedUnexpectedDwxNotify

Recovery:

1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact *My Oracle Support (MOS).*

22310 - Received Unexpected DPR/DPA

Event Type: DIAM

Description: DPR or DPA message was received from the peer when it was not expected.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedUnexpectedDpxNotify

Recovery:

1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact *My Oracle Support (MOS).*

22311 - Invalid Diameter message received

Event Type: DIAM

Description: Diameter message received from peer which was decodable but contained a semantic error.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedInvalidDiameterMessageNotify

Recovery:

1. Analyze MsgOctets to determine which semantic error occurred and diagnose peer for unexpected behavior.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22312 - Socket send failure

Event Type: DIAM

Description: An unexpected error occurred during the socket send call when attempting to send a Diameter message to the peer.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterFailedToSendDiameterMessageNotify

Recovery:

1. Analyze error value to determine root cause.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22313 - Connection Unavailable: Transport failure

Event Type: DIAM

Description: The connection was closed by the SCTP or TCP transport.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailTransportFailureNotify

Recovery:

1. Analyze error value to determine root cause.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22314 - Connection Unavailable: CEA Realm/Host validation failure

Event Type: DIAM

Description: Origin-Realm and/or Origin-Host in CEA message received from peer on locally initiated connection does not match the locally configured connection.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailCeaRealmHostVldtnFailNotify

Recovery:

1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration using the **Diameter** > **Configuration** > **Local Nodes** page.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22316 - Connection Unavailable: No common apps

Event Type: DIAM

Description: No common applications were found between local node and peer node during capabilities exchange.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailNoCommonAppsNotify

Recovery:

1. Reconcile Application IDs between local and peer nodes. If no common applications exist, the connection should be deleted or Disabled.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22319 - Connection Unavailable: Diameter Watchdog

Event Type: DIAM

Description: Connection closed due to no traffic from peer within Tw*2 time after sending DWR.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailWatchdogFailureNotify

Recovery:

1. Confirm that the connection is not administratively Disabled at the peer.
2. Confirm that the peer connection configuration (protocol, remote/local IP address, remote/local port) matches local connection configuration.
3. Confirm there is reliable IP network connectivity between the peer IP and the local IP for the connection (no excess packet loss).
4. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22320 - Invalid peer initiated connection

Event Type: DIAM

Description: Origin-Realm and or Origin-Host in CER message received or the peer IP addresses advertised on peer initiated connection does not match any locally configured connection

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterInvalidPeerInitdConnNotify

Recovery:

1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22321 - Connection Unavailable: DNS Resolution Failure

Event Type: DIAM

Description: During connection initiation, Transport/Peer FQDN was unable to be resolved to an IP address via DNS

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailDnsResolutionFailureNotify

Recovery:

1. Confirm DNS is available and reachable by MP.
2. Confirm that DNS configuration contains peer FQDN and appropriate corresponding IP address(es).
3. Analyze errno value and text from Event Addn'l Info to determine root cause.
4. If the problem persists, contact *My Oracle Support (MOS)*.

22322 - Connection Proving Success

Event Type: DIAM

Description: The connection proving phase completed successfully.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnProvingSuccessNotify

Recovery:

No action required.

22323 - Connection Degraded: Diameter Watchdog

Event Type: DIAM

Description: Connection declared suspect due to no traffic from peer within Tw time after sending DWR.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterConnDegradedWatchdogSuspectNotify

Recovery:

1. Examine the peer to determine why it is not responding.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22326 - Connection Established

Event Type: DIAM

Description: The peer connection is available for signaling traffic.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnEstablishedNotify

Recovery:

No action required.

22327 - Initiator function disabled

Event Type: DIAM

Description: Peer disconnect reason indicated that we should not attempt to initiate a connection.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterInitiatorFunctionDisabledNotify

Recovery:

1. No action required. The peer can still initiate a connection. If the peer does not attempt to initiate a connection within a reasonable amount of time, the connection can be disabled, then re-enabled to re-activate the initiator function.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22328 - Connection is processing a higher than normal ingress messaging rate

Alarm Group: DIAM

Description: The diameter connection specified in the alarm instance is processing a higher than normal ingress messaging rate.

Severity:

- Minor (if all of the following are true):
  - The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection minor alarm threshold.
  - The average ingress MPS rate that the connection is processing has not yet reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

- Major (if the following are true):
  - The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

Instance: The name of the diameter connection as defined by the TransportConnection table.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIngressMpsRateNotify

Recovery:

1. The Diameter connection specified in the Alarm Instance field is processing a higher than expected average ingress Diameter message rate. The alarm thresholds for minor and major alarms are configured in the Capacity Configuration Set used by the Diameter connection.
2. The message rate used for this alarm is an exponentially smoothed 30 second average. This smoothing limits false alarms due to short duration spikes in the ingress message rate.
3. If the alarm severity is minor, the alarm means that the average ingress message rate has exceeded the minor alarm threshold percentage of the maximum ingress MPS configured for the connection.
4. If the alarm severity is major, the alarm means that the average ingress message rate has exceeded the major alarm threshold percentage of the maximum ingress MPS configured for the connection.
5. This alarm is cleared when the average ingress message rate falls 5% below the minor alarm threshold, or the connection becomes disabled or disconnected. This alarm is downgraded from major to minor if the average ingress message rate falls 5% below the major alarm threshold.
6. If the average ingress message rate is determined to be unusually high, investigate the connection's remote Diameter peer (the source of the ingress messaging) to determine why they are sending the abnormally high traffic rate. Otherwise, consider increasing either the connection's maximum ingress MPS rate or the connection's alarm thresholds.

22329 - SCTP Connection Impaired: A path has become unreachable

Event Type: DIAM

Description: A path of an established SCTP connection has become unreachable.

Severity: Info

Instance: <TransConnName:Peer IP> (peer/remote IP of the failed path)

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSctpConnectionImpairedNotify

Recovery:

1. Check whether the routing path between the local IP address and the peer IP address is up. If it is not, fix it.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22330 - SCTP Connection Cfg Mismatch: The peer advertised a different number of IP addresses than configured

Event Type: DIAM

Description: The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterSctpConnectionCfgMismatchNotify

Recovery:

Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the **Diameter > Configuration > System Options** page.

22331 - SCTP Connection Partial Matching: SCTP connection accepted but the IP addresses advertised by the peer match only partially those configured for the peer in the connection object

Event Type: DIAM

Description: The peer has advertised in the INIT/INIT_ACK chunk a set of IP addresses which overlap but does not include all the IP addresses configured for the peer in the respective connection object.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterSCTPConnectionPartialMatchingNotify

Recovery:

1. Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the **Diameter > Configuration > System Options** page.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22332 - Connection Rejected: Max Connections Exceeded

Event Type: DIAM

Description: Connection was rejected due to the DA-MP exceeding its maximum number of supported Diameter Connections.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnRejMaxConnExceededNotify

Recovery:

1. If the DA-MP is a member of a IPFE TS, verify that the IPFE is configured to fully monitor the DA-MP's availability status.

   When a IPFE fully monitors application servers in a IPFE TS, it will cease from distributing new Diameter connections to any/all application servers that report a "Stasis" availability status.

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

22334 - Unexpected Message Priority in ingress Request

Event Type: DIAM

Description: The decoded Message Priority from the ingress Request has an unexpected value.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterUnexpMessagePriorityInRequestNotify

Recovery:

1. Verify that the peer is a DSR

   * Product-Name is reported as "Eagle XG DSR", in the Event Additional Information.
   * Vendor-Id is reported as 323 (Tekelec).

2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.

   * Call *My Oracle Support (MOS)* and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   * If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call *My Oracle Support (MOS)*.
   * If the reported Firmware-Version is less than the minimum required DSR software version, call *My Oracle Support (MOS)* to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to "None".

22335 - Peer does not support Message Priority

Event Type: DIAM

Description: Cannot read Message Priority from ingress Requests because Peer does not support Message Priority.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterMessagePriorityNotSuppPeerNotify

Recovery:

1. Verify that the peer is a DSR

    *   Product-Name is reported as "Eagle XG DSR", in the Event Additional Information.
    *   Vendor-Id is reported as 323 (Tekelec).

2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.

    *   Call *My Oracle Support (MOS)* and obtain the minimum DSR software version that supports Message Priority and compare with this information.
    *   If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call *My Oracle Support (MOS)*.
    *   If the reported Firmware-Version is less than the minimum required DSR software version, call *My Oracle Support (MOS)* to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to "None".

22343 - Connection Unavailable: Duplicate Connection Released

Event Type: DIAM

Description: Duplicate connection established, connection terminated.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterDuplicateConnectionReleasedNotify

Recovery:

No action necessary.

22344 - Failed to process ingress message: Processor Unavailable or Congested

Event Type: DIAM

Description: The message processor is Unavailable or Congested. This event refers to another DA-MP, not the one reporting the problem.

Severity: Info

Instance: <SourceMpHost>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterProcessorUnavlblOrCngstedNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22345 - Connection Priority Level changed

Event Type: DIAM

Description: The Diameter Connection's CPL has transitioned from its current value to a new CPL value based on congestion levels reported by various features.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterCplChangedNotify

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Identify the most recent "Connection Degraded" event in the event log for the connection and utilize the Event Detailed information to diagnose the condition.
3. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

22346 - MP Reserved Ingress MPS Oversubscribed

Event Type: DIAM

Description: The total connection Reserved Ingress MPS exceeds the Engineered Ingress MPS capacity of the MP.

Severity: Info

Instance: MPName (Hostname of the DA-MP Server)

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterMpResIngressMpsOversubscribedNotify

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Perform one or more of these actions:

- Increase the maximum reserved capacity by increasing the value of IPFE Connection Reserved Ingress MPS Scaling parameter.
- Reduce the subscribed amount of reserved capacity by reducing the number of connections.
- Reduce the reserved capacity required by connections.

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

22347 - Ingress Message Discarded: DA-MP shared ingress capacity exhausted

Alarm Group: DIAM

Description: An ingress message is discarded on a DA-MP due to the ingress message rate on the DA-MP exceeding MP Maximum Ingress MPS.

Severity: N/A

Instance: <MPHostName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressMessageDiscardedNotify

Recovery:

1. The ingress MPS on the DA-MP is exceeding the MP Maximum Ingress MPS. Consider decreasing the overall ingress message rate on the DA-MP by diverting the traffic or reducing the traffic.
2. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

22349 - IPFE Connection Alarm Aggregation Threshold

Alarm Group: DIAM

Description: This alarm occurs when there are a 'Critical' number of IPFE Connection alarms for the Network Element.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical, Major

Note: The Critical threshold may be disabled by setting the Critical Threshold to zero using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIPFEConnUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Connection** to monitor IPFE Connection status.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.

3. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.

4. Verify that the peers in the Route List are not under maintenance.

5. Contact *My Oracle Support (MOS)* for assistance.

22350 - Fixed Connection Alarm Aggregation Threshold

Alarm Group: DIAM

Description: This alarm occurs when there are a 'Critical' number of Fixed Connection alarms for the DA-MP.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical, Major

Note: The Critical threshold may be disabled by setting the Critical Threshold to zero using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Instance: <DA-MP-Hostname>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Connection** to monitor Fixed Connection status.

2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.

3. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.

4. Verify that the peers in the Route List are not under maintenance.

5. Contact *My Oracle Support (MOS)* for assistance.

22900 - DPI DB Table Monitoring Overrun

Event Type: DIAM

Description: The COMCOL update sync log used by DB Table monitoring to synchronize Diameter Connection Status among all DA-MP RT-DBs has overrun. The DA-MP's Diameter Connection Status sharing table is automatically audited and re-synced to correct any inconsistencies.

Severity: Info

Instance: <DbTblName>

Note: <DbTblName> refers to the name of the Diameter Connection Status Sharing Table the Diameter Connection status inconsistency that was detected.

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDpiTblMonCbOnLogOverrunNotify

Recovery:

Contact *My Oracle Support (MOS)* if this alarm is constantly being asserted and cleared.

22901 - DPI DB Table Monitoring Error

Event Type: DIAM

Description: An unexpected error occurred during DB Table Monitoring.

Severity: Info

Instance: DpiTblMonThreadName

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDpiSldbMonAbnormalErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

22950 - Connection Status Inconsistency Exists

Alarm Group: DIAM

Description: Diameter Connection status inconsistencies exist among the DA-MPs in the DSR signaling NE.

Severity: Critical

Instance: <MpName> (where inconsistency detected)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnStatusInconsistencyExistsNotify

Recovery:

No action necessary.

Note: DA-MP's SLDB tables are automatically audited and re-synchronized to correct inconsistencies after a log overrun has occurred.

22960 - DA-MP Profile Not Assigned

Alarm Group: DIAM

Description: A DA-MP configuration profile has not been assigned to this DA-MP.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDaMpProfileNotAssignedNotify

Recovery:

1. A DA-MP profile must be assigned to the DA-MP via the DSR OAM GUI.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22961 - Insufficient Memory for Feature Set

Alarm Group: DIAM

Description: The Available Memory (in kilobytes) for Feature Set is less than the Required Memory (in kilobytes).

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterInsufficientAvailMemNotify

Recovery:

1. Make additional memory available on the DA-MP for the configured DiameterMaxMessageSize.
2. If the problem persists, contact *My Oracle Support (MOS)*.

Range Based Address Resolution (RBAR) Alarms and Events (22400-22424)

22400 - Message Decoding Failure

Event Type: RBAR

Description: A message received was rejected because of a decoding failure.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarMsgRejectedDecodingFailureNotify

Recovery:

While parsing the message, the message content was inconsistent with the Message Length in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

22401 - Unknown Application ID

Event Type: RBAR

Description: A message could not be routed because the Diameter Application ID is not supported.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarUnknownApplIdNotify

Recovery:

1. The DSR Relay Agent forwarded a Request message to the address resolution application which contained an unrecognized Diameter Application ID in the header. Either a DSR Relay Agent application routing rule is mis-provisioned or the Application ID is not provisioned in the RBAR routing configuration.
2. View the currently provisioned Diameter Application IDs by selecting **RBAR** > **Configuration** > **Applications**.
3. View the currently provisioned Application Routing Rules by selecting **Diameter** > **Configuration** > **Application Routing Rules**.

22402 - Unknown Command Code

Event Type: RBAR

Description: A message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarUnknownCmdCodeNotify

Recovery:

1. The order pair (Application ID, Command Code) is not provisioned in the Address Resolutions routing configuration.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22403 - No Routing Entity Address AVPs

Event Type: RBAR

Description: A message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarNoRoutingEntityAddrAvpNotify

Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22404 - No valid Routing Entity Addresses found

Event Type: RBAR

Description: A message could not be routed because none of the address AVPs contained a valid address and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarNoValidRoutingEntityAddrFoundNotify

Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22405 - Valid address received didn't match a provisioned address or address range

Event Type: RBAR

Description: A message could not be routed because a valid address was found that did not match an individual address or address range associated with the Application ID, Command Code, and Routing Entity Type, and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarAddrMismatchWithProvisionedAddressNotify

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22406 - Routing attempt failed due to internal resource exhaustion

Event Type: RBAR

Description: A message could not be routed because the internal "Request Message Queue" to the DSR Relay Agent was full. This should not occur unless the MP is experiencing local congestion as indicated by Alarm-ID *22200 - Local MP Congestion*.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarRoutingAttemptFailureInternalResExhNotify

Recovery:

> If this problem occurs, contact *My Oracle Support (MOS)*.

22407 - Routing attempt failed due to internal database inconsistency failure

Event Type: RBAR

Description: A message could not be routed because an internal address resolution run-time database inconsistency was encountered.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarRoutingFailureInternalDbInconsistencyNotify

Recovery:

> If this problem occurs, contact *My Oracle Support (MOS)*.

Generic Application Alarms and Events (22500-22599)

Note: These alarms are generic across the various DSR applications with some details varying depending on the application generating the alarm.

22500 - DSR Application Unavailable

Alarm Group: APPL

Description: DSR Application is unable to process any messages because it is Unavailable

Severity: Critical

Instance: <DSR Application Name>

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationUnavailableNotify

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify that the Admin State is set as expected.
2. A DSR Application operation status becomes Unavailable when either the Admin State is set to Disable with the Forced Shutdown option, or the Admin State is set to Disable with the Graceful Shutdown option and the Graceful Shutdown timer expires.
3. A DSR Application can also become Unavailable when it reaches Congestion Level 3 if enabled.

   Note: This alarm will NOT be raised when the DSR application is shutting down gracefully or application is in Disabled state. Only the DSR Application operational status will be changed to Unavailable.

4. Check the Event History logs for additional DIAM events or alarms for this MP server.
5. If the problem persists, contact *My Oracle Support (MOS)*.

22501 - DSR Application Degraded

Alarm Group: APPL

Description: Unable to forward requests to the DSR Application because it is Degraded

Severity: Major

Instance: <DSR Application Name>

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, PCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationDegradedNotify

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify that the Admin State is set as expected.

2. A DSR Application becomes Degraded when the DSR Application becomes congested if enabled.

   Note: This alarm will NOT be raised when the DSR application is shutting down gracefully or application is in Disabled state. Only the DSR Application operational status will be changed to Unavailable.

3. Check the Event History logs for additional DIAM events or alarms for this MP server.

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

22502 - DSR Application Request Message Queue Utilization

Alarm Group: APPL

Description: The DSR Application Request Message Queue Utilization is approaching its maximum capacity

Severity:

- **Minor:** Request Queue utilization becomes over 60%
- **Major:** Request Queue utilization becomes over 80%
- **Critical:** Request Queue utilization becomes over 95%

Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraRequestMsgQueue, RxCpaRequestMsgQueue for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, PCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationRequestQueueUtilNotify

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify that the Admin State is set as expected.

   The DSR Application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.

2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.

3. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Request Message Queue. Examine the Alarm log in **Alarms & Events**

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

22503 - DSR Application Answer Message Queue Utilization

Alarm Group: APPL

Description: The DSR Application Answer Message Queue Utilization is approaching its maximum capacity.

Severity:

- **Minor:** Answer Queue utilization becomes over 60%
- **Major:** Answer Queue utilization becomes over 80%
- **Critical:** Answer Queue utilization becomes over 95%

Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraAnswerMsgQueue, RxCpaAnswerMsgQueue for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, PCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationAnswerQueueUtilNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules** in the SO GUI.

2. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Answer Message Queue. Examine the Alarm log in **Alarms & Events**

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

22504 - DSR Application Ingress Message Rate

Alarm Group: APPL

Description: The ingress message rate for the DSR Application is exceeding its engineered traffic handling capacity.

Severity:

- **Minor:** Ingress Message Rate becomes over 110% of the ingress message capacity

- **Major:** Ingress Message Rate becomes over 140% of the ingress message capacity
- **Critical:** Ingress Message Rate becomes over 160% of the ingress message capacity

Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraMsgRate, RxCpaMsgRate for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, PCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationIngressMsgRateNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules** in the SO GUI.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, contact *My Oracle Support (MOS)*.

22520 - DSR Application Enabled

Event Type: APPL

Description: DSR Application Admin state was changed to 'enabled'.

Severity: Info

Instance: <DSR Application Name>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationEnabledNotify

Recovery:

No action required.

22521 - DSR Application Disabled

Event Type: APPL

Description: DSR Application Admin state was changed to 'disabled'.

Severity: Info

Instance: <DSR Application Name>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationDisabledNotify

Recovery:

No action required.

Full Address Based Resolution (FABR) Alarms and Events (22600-22640)

22600 - Message Decoding Failure

Event Type: FABR

Description: Message received was rejected because of a decoding failure. While parsing the message, the message content was inconsistent with the "Message Length" in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message), the peer who forwarded the message to this node, or any intermediate node that modifies the message.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrMsgRejectedDecodingFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22601 - Unknown Application ID

Event Type: FABR

Description: Message could not be routed because the Diameter Application ID is not supported.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrUnknownApplIdNotify

Recovery:

A Request message was forwarded to the FABR application which contained an unrecognized Diameter Application ID in the header. Either an application routing rule is mis-provisioned or the Application ID is not provisioned in the FABR configuration.

1. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**

2. The currently provisioned Diameter Application IDs can be viewed in the **FABR** > **Configuration** > **Applications Configuration**.

3. Contact *My Oracle Support (MOS)* for assistance.

22602 - Unknown Command Code

Event Type: FABR

Description: Message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrUnknownCmdCodeNotify

Recovery:

Either an application routing rule is mis-provisioned or the Command Code is not provisioned in the FABR configuration.

1. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**

2. The currently provisioned Diameter Application IDs can be viewed in the **FABR** > **Configuration** > **Address Resolutions**.

3. Contact *My Oracle Support (MOS)* for assistance.

22603 - No Routing Entity Address AVPs

Event Type: FABR

Description: Message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrNoRoutingEntityAddrAvpNotify

Recovery:

1. If this event is considered abnormal, then validate which AVPs are configured for routing with the Application ID and Command Code using **FABR** > **Configuration** > **Address Resolutions**.

2. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**

3. Contact *My Oracle Support (MOS)* for assistance.

22604 - No valid User Identity Addresses found

Event Type: FABR

Description: No valid User Identity Address is found in the configured AVPs contained in the ingress message.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrNoValidUserIdentityAddrFoundNotify

Recovery:

1. If this event is considered abnormal, then validate which AVPs are configured for routing with the Application ID and Command Code using **FABR** > **Configuration** > **Address Resolutions**.

2. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**

3. Contact *My Oracle Support (MOS)* for assistance.

22605 - No Destination address is found to match the valid User Identity address

Event Type: FABR

Description: Message could not be routed because the valid user identity address extracted from the message did not resolve to a destination address. The Routing Exception was configured to send an Answer response. Please verify the provisioning in the address resolution table and the data provided in the SDS corresponding to this address/resolution entry.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrNoAddrFoundAtDpNotify

Recovery:

The FABR address resolution table entry may be misconfigured or the destination address associated with User Identity address from the message and the destination type configured in the address resolution table may be missing from the address mapping configuration. The destination address

associated with User Identity address derived may be missing from the address mapping configuration on DP/SDS.

1. Validate the address resolution table entry and verify that a valid destination address is associated with the user identity address by using DP configuration.

   For additional information, see Subscriber Database Server online help.

2. Contact *My Oracle Support (MOS)* for assistance.

22606 - Database or DB connection error

Event Type: FABR

Description: FABR application receives service notification indicating Database (DP) or DB connection (ComAgent) Errors (DP timeout, errors or ComAgent internal errors) for the sent database query.

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrDpErrorsNotify

Recovery:

   Contact *My Oracle Support (MOS)* for assistance.

22607 - Routing attempt failed due to DRL queue exhaustion

Event Type: FABR

Description: Message could not be routed because the internal "Request Message Queue" to the DSR Relay Agent was full.

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrRoutingAttemptFailureDrlQueueExhNotify

Recovery:

   Contact *My Oracle Support (MOS)* for assistance.

22608 - Database query could not be sent due to DB congestion

Event Type: FABR

Description: FABR could not send a database query either because the ComAgent reported DP congestion level of (CL=2 or 3), or an abatement period is in progress.

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrDpCongestedNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22609 - Database connection exhausted

Event Type: FABR

Description: Database queries could not be sent because the database connection (ComAgent) queue was full

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrDbConnectionExhNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22610 - FABR DP Service congestion state change

Event Type: FABR

Description: FABR application received status notification indicating DP congestion state change or DP congestion abatement time period has completed.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterFabrDpCongestionStateChangeNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22611 - FABR Blacklisted Subscriber

Event Type: FABR

Description: Message could not be routed because valid User Identity Address extracted from diameter request belongs to blacklisted subscriber.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrBlacklistedSubscriberNotify

Recovery:

The destination address associated with User Identity address derived is blacklisted in the address mapping configuration on DDR.

1. Validate which User identity address is not blacklisted by using DP configuration.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22631 - FABR DP Response Task Message Queue Utilization

Alarm Group: FABR

Description: The FABR Application's DP Response Message Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxFabrDpResponseMsgQueue, FABR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterFabrAppDpResponseMessageQueueUtilizationNotify

Recovery:

1. This alarm may occur due to persistent overload conditions with respect to database response processing.
2. Contact *My Oracle Support (MOS)* for assistance.

22632 - COM Agent Registration Failure

Alarm Group: FABR

Description: The Communication Agent routing service registration or service notification registration failed, FABR can not use the Communication Agent service for database queries.

Severity: Critical

Instance: Full Address Based Resolution

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterComAgentRegistFailNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

Policy and Charging Application (PCA) Alarms and Events (22700-22799)

22700 - Protocol Error in Diameter Requests

Event Group: PCA

Description: The Diameter Request message(s) received by PCA contain protocol error(s).

Severity: Info

Instance: PCA, Policy DRA, Online Charging DRA

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraProtocolErrorsInDiameterReqNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22701 - Protocol Error in Diameter Answers

Event Group: PCA

Description: The Diameter Answer message(s) received by PCA contain(s) protocol error(s). This error message is based on error scenarios such as:

- Command-Code value is not supported
- Mandatory AVP used for processing decisions is missing
- Mandatory AVP used for processing contains an invalid value
- Mandatory Session-Id AVP has a zero-length value

Note: This event is not generated when the received Diameter Answer message 'E' (Error) bit is set and a mandatory Diameter command-specific AVP (AVPs other than Session-ID, Origin-Host, Origin-Realm, and result-Code) are missing.

Severity: Info

Instance: PCA, Policy DRA, Online Charging DRA

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraProtocolErrorsInDiameterAnsNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22702 - Database Hash Function Error

Event Type: PCA

Description: The hash function result does not map to a database resource or sub-resource

Severity: Info

Instance: N/A

HA Score: Normal

OID: pdraPdraHashingResDoesNotMatchResOrSubResNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22703 - Diameter Message Routing Failure Due To Full DRL Queue

Event Type: PCA

Description: The Diameter Egress message could not be sent because the DRL Message Queue is full.

Severity: Info

Instance: PCA, Policy DRA, Online Charging DRA

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraEgressMsgRoutingFailureDueToDrlQueueExhaustedNotify

Recovery:

1. Refer to measurement RxGyRoAnsDiscardDrlQueueFullPerCmd (in the *DSR Measurements Reference)* to determine the number of Gy/Ro Diameter Credit Control Application Answer messages discarded by OC-DRA due to DRL's Answer queue being full.
2. Contact *My Oracle Support (MOS)* for assistance.

22704 - Communication Agent Error

Event Type: PCA

Description: The Policy and Charging server to SBR server communication failure.

Severity: Policy DRA, Online Charging DRA

Instance: Info

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraStackEventSendingFailureCAUnavailNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22705 - SBR Error Response Received

Event Type: PCA

Description: The Policy and Charging server received response from SBR server indicating SBR errors.

Severity: Info

Instance: Policy DRA, Online Charging DRA

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraPsbrErrorIndicationNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22706 - Binding Key Not Found In Diameter Message

Event Type: PCA

Description: A binding key is not found in the received CCR-I message.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraBindingKeyNotFoundNotify

Recovery:

1. Check the P-DRA GUI at **Policy DRA** > **Configuration** > **Binding Key Priority**.
2. Contact *My Oracle Support (MOS)* for assistance

22707 - Diameter Message Processing Failure

Alarm Group: PCA

Description: PCA failed to process a Diameter message. The specific reason is provided by the PCA signaling code.

Severity: Info

Instance: Policy DRA, Online Charging DRA

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraDiameterMessageProcessingFailureNotify

Recovery:

1. If the event was generated for a Diameter message being discarded due to congestion, refer to the Recovery steps for Alarm *22504 - DSR Application Ingress Message Rate*.

2. Contact *My Oracle Support (MOS)* for further assistance.

22708 - PCA Function is Disabled

Alarm Group: PCA

Description: The PCA Function is unable to process any messages because it is Disabled.

Severity: Major

Instance: Policy DRA, Online Charging DRA

HA Score: Normal

Auto Clear Seconds: 60

OID: pdraPcaFunctionDisabledNotify

Recovery:

1. The PCA Function becomes Disabled when the Admin State is set to Disable. The PCA Function Admin State can be determined from the SOAM GUI **Main Menu** > **Policy and Charging** > **General Options**. Verify the admin state is set as expected.

2. If the Admin State of the PCA Function is to remain Disabled, consider changing the ART configuration to stop sending traffic for that function to PCA.

3. Contact *My Oracle Support (MOS)* for assistance if needed.

22709 - PCA Function is Unavailable

Alarm Group: PCA

Description: The PCA Function is unable to process any messages because it is Unavailable.

Severity: Major

Instance: PcaFunctionName

HA Score: Normal

Auto Clear Seconds: 0

OID: pdraPcaFunctionUnavailableNotify

Recovery:

1. The availability of the Policy DRA function to receive and process ingress messages is based on its administration state (Enabled or Disabled) and the status of the SBR Binding and Session resources.

2. The availability of the Online Charging DRA function to receive and process ingress messages is based on its administration state (Enabled or Disabled), OCS configuration, and the status of the SBR Session resource.

3. The PCA function is unavailable to receive and process ingress messages for one of the following reasons:

- "Insufficient Binding SBR Resources" - the number of Binding SBR sub-resources available is less than the minimum number required. Refer to the Recovery steps for Alarm *22722 - Policy Binding Sub-resource Unavailable*, which will also be asserted.
- "Insufficient Session SBR Resources" - the number of Session SBR sub-resources available is less than the minimum number required. Refer to the Recovery steps for Alarm *22723 - Policy and Charging Session Sub-resource Unavailable*, which will also be asserted.
- "No OCSs Configured at Site" - At least one OCS is required to be locally configured. Use the SOAM GUI Main Menu **Policy and Charging** > **Configuration** > **Online Charging DRA** > **OCSs** to configure an OCS at the site.

4. Contact *My Oracle Support (MOS)* for assistance if needed.

22710 - SBR Sessions Threshold Exceeded

Alarm Group: SBR

Description: The number of SBR sessions threshold for a Policy and Charging Mated Sites Place Association has been exceeded.

Severity:

- **Minor**: SBR session numbers are greater than or equal to 80% of maximum session capacity
- **Major**: SBR session numbers are greater than or equal to 90% of maximum session capacity
- **Critical**: SBR session numbers are greater than or equal to 95% of maximum session capacity

Instance: Policy and Charging Mated Sites Place Association Name

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPsbrActSessThreshNotify

Recovery:

1. The session database associated with the Policy and Charging Network Mated Sites Place Association specified in the Instance field is nearing the limit on the number of session records. The alarm thresholds for Session Capacity alarms are configured network wide on the Network OAM from the **Policy and Charging** > **Configuration** > **Alarm Settings** screen.
Alarm severity is determined by the number of session records stored in the policy session database exceeding the alarm threshold percentage of the calculated session capacity for the topology.
2. If the alarm assert thresholds are improperly configured, they can be configured on a network-wide basis from the Network OAM Gui Main menu from **Policy DRA** > **Configuration** > **Alarm Settings**.
3. In general, the system should be sized to host the expected number of concurrent sessions per policy subscriber.
4. If the system is nearing 100% capacity, contact *My Oracle Support (MOS)* for further assistance.

22711 - SBR Database Error

Alarm Group: SBR

Description: An error occurred during a SBR database operation.

Severity: Info

Instance: Binding SBR, Session SBR

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterPSBRDbOpFailNotify

Recovery:

1. An unexpected, internal error was encountered while the SBR database was being accessed. This error may occur for a variety of reasons:

    1. The database is filled to capacity
    2. Database inconsistency between NO and SO tables caused by a database restore operation. This issue is corrected by the SBR audit.

2. Contact *My Oracle Support (MOS)* for further assistance.

22712 - SBR Communication Error

Alarm Group: SBR

Description: The SBR received an error or timeout response from Communication Agent for a non-audit stack event.

Severity: Info

Instance: Binding SBR, Session SBR

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterPSBRStkEvFailComAgentNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22713 - SBR Alternate Key Creation Error

Alarm Group: SBR

Description: Failed to create an Alternate Key record in the Binding database.

Severity: Info

Instance: Session SBR

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterPSBRAltKeyCreateFailNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22714 - SBR RAR Initiation Error

Alarm Group: SBR

Description: SBR encountered an error while processing PCA initiated RAR requests.

Severity: Info

Instance: Session SBR

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterPSBRRARInitiationErrNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22715 - SBR Audit Suspended

Alarm Group: SBR

Description: SBR binding and/or session auditing has been suspended due to a congestion condition on either the local server reporting the alarm, or on a remote server being queried for auditing purposes

Severity: Minor

Instance: Session SBR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSBRAuditSuspendedNotify

Recovery:

1. The audit cleans up stale records in the database. Prolonged suspension of the audit could result in the exhaustion of memory resources on a binding or session SBR server. Investigate the causes of congestion on the SBR servers (see also 22725).
2. If the problem persists, contact *My Oracle Support (MOS)*.

22716 - SBR Audit Statistics Report

Event Group: SBR

Description: This report provides statistics related to SBR session or binding table audits. Each SBR server generates this event upon reaching the last record in a table. The statistics reported are appropriate for the type of table being audited. This report also provides hourly statistics related to the Pending RAR report.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 0 (no throttling)

OID: eagleXgDiameterPSBRAuditStatisticsReportNotify

Recovery:

Contact *My Oracle Support (MOS)*.

22717 - SBR Alternate Key Creation Failure Rate

Alarm Group: SBR

Description: SBR Alternate Key Creation Failure rate exceeds threshold.

Severity: Minor, Major, Critical

Instance: PsbrAltKeyCreationFailureRate, SBR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSBRAltKeyCreationFailureRateNotify

Recovery:

If the further assistance is needed, contact *My Oracle Support (MOS)*.

22718 - Binding Not Found for Binding Dependent Session Initiate Request

Event Group: PCA

Description: Binding record is not found for the configured binding keys in the binding dependent session-initiation request message.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraBindingRecordNotFoundNotify

Recovery:

1. Check the Policy and Charging GUI Main Menu **Policy and Charging** > **Configuration** > **Binding Key Priority** on the subscriber key priorities to ensure the configuration is correct.
2. Using the Binding Key Query Tool, check if a binding exists for the binding keys at **Policy DRA** > **Configuration** > **Binding Key Priority**.

22719 - Maximum Number of Sessions per Binding Exceeded

Event Group: PCA

Description: A Binding capable session initiation request failed because this subscriber already has the maximum number of sessions per binding

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraMaxSessionsReachedNotify

Recovery:

1. Determine if the existing sessions are valid. The existing sessions may be displayed using the Binding Key Query Tool to obtain all relevant information including session-ids and PCEF FQDNs.
2. If the sessions exist in the P-DRA but not on the PCEF(s), call the *My Oracle Support (MOS)*.

22720 - Policy SBR To PCA Response Queue Utilization Threshold Exceeded

Alarm Group: PCA

Description: The SBR to PCA Response Queue Utilization Threshold Exceeded

Severity:

- **Minor**: SBR Response Queue Utilization becomes over 60%
- **Major**: SBR Response Queue Utilization becomes over 80%
- **Critical**: SBR Response Queue Utilization becomes over 95%

Instance: RxPcaSbrEventMsgQueue, PCA

HA Score: Normal

OID: pdraPdraPsbrResponseQueueUtilizationNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**

   Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, contact *My Oracle Support (MOS)*.

22721 - Policy and Charging Server In Congestion

Alarm Group: PCA

Description: The Policy and Charging Server is operating in congestion.

Severity:

- **Minor**: ingress Request rate is 110% of ingress request message capacity or larger
- **Major**: ingress Request rate is 140% of ingress request message capacity or larger
- **Critical**: ingress Request rate is 160% of ingress request message capacity or larger

Instance: PCA

HA Score: Normal

OID: pdraPdraCongestionStateNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

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

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

22722 - Policy Binding Sub-resource Unavailable

Alarm Group: PCA

Description: One or more Policy binding sub-resources are not available.

Severity:

- **Major**: When Policy DRA function is enabled and at least one server group that has a range of binding sub-resources is not available
- **Critical**: When Policy DRA function is enabled and all of the binding sub-resources are not available, i.e. all server groups hosting the sub-resources are not available.

Instance: N/A

HA Score: Normal

OID: pdraPdraBindingSubresourceUnavailableNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Look for ComAgent connectino Alarms. If ComAgent connection alarms exist, follow the Recovery steps for those alarms to troubleshoot further. If there are no ComAgent connection alarms, review the configuration of Resource Domains, Places, and Place Associations using the NOAM GUI and verify that they are provisioned as expected:

   - **Main Menu** > **Configuration** > **Resource Domains**
   - **Main Menu** > **Configuration** > **Places**
   - **Main Menu** > **Configuration** > **Place Associations**

2. Navigate to the ComAgent HA Services Status screen at **Main Menu** > **Communication Agent** > **Maintenance** > **HA Service Status**and locate the Resource with name equal to that configured as the Resource Domain for the SBR Database.

3. Click the HA Services Status row for the Resource, which will have further detailed information about the Communication Agent's problem.

4. Contact *My Oracle Support (MOS)* for assistance if needed.

22723 - Policy and Charging Session Sub-resource Unavailable

Alarm Group: PCA

Description: One or more Policy and Charging session sub-resources are not available.

Severity:

- **Major**: When Policy DRA and/or Online Charging DRA are enabled and at least one of the server groups hosting session sub-resources is not available.
- **Critical**: When Policy DRA and/or Online Charging DRA are enabled and all of the server groups hosting session sub-resources are not available.

Instance: Policy DRA

HA Score: Normal

OID: pdraPdraSessionSubresourceUnavailableNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Look for ComAgent connectino Alarms. If ComAgent connection alarms exist, follow the Recovery steps for those alarms to troubleshoot further. If there are no ComAgent connection alarms, review the configuration of Resource Domains, Places, and Place Associations using the NOAM GUI and verify that they are provisioned as expected:

    - **Main Menu** > **Configuration** > **Resource Domains**
    - **Main Menu** > **Configuration** > **Places**
    - **Main Menu** > **Configuration** > **Place Associations**

2. Navigate to the ComAgent HA Services Status screen at **Main Menu** > **Communication Agent** > **Maintenance** > **HA Service Status**and locate the Resource with name equal to that configured as the Resource Domain for the SBR Database.

3. Click the HA Services Status row for the Resource, which will have further detailed information about the Communication Agent's problem.

4. Contact *My Oracle Support (MOS)* for assistance if needed.

22724 - SBR Memory Utilization Threshold Exceeded

Alarm Group: SBR

Description: The SBR server memory utilization threshold has been exceeded.

Severity:

- **Minor**: SBR memory utilization threshold exceeds 70%

- **Major**: SBR memory utilization threshold exceeds 80%
- **Critical**: SBR memory utilization threshold exceeds 90%

Instance: psbr.MemPerTotal, SBR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrMemUtilNotify

Recovery:

1. If this condition persists, it may be necessary to allocate more memory for SBR.
2. Contact *My Oracle Support (MOS)* for further assistance.

22725 - SBR Server In Congestion

Alarm Group: SBR

Description: The SBR server is operating in congestion.

Severity:

- **Minor:** CL_1
- **Major:** CL_2
- **Critical:** CL_3

Instance: Policy and Charging mated Sites Place Association Name

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterFPSbrServerInCongestionNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

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

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

22726 - SBR Queue Utilization Threshold Exceeded

Alarm Group: SBR

Description: The SBR stack event queue utilization threshold has been exceeded.

Severity:

- **Minor**: SBR stack event queue utilization threshold exceeds 60%
- **Major**: SBR stack event queue utilization threshold exceeds 80%
- **Critical**: SBR stack event queue utilization threshold exceeds 95%

Instance: psbr.MemPerTotal, SBR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrStackEvQUtilNotify

Recovery:

1. If this condition persists, it may be necessary to allocate larger queue sizes.
2. Contact *My Oracle Support (MOS)* for further assistance.

22727 - SBR Initialization Failure

Alarm Group: SBR

Description: The SBR server process failed to initialize.

Severity: Critical

Instance: Policy DRA Mated Sites Place Association Name

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrInitializationFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

22728 - SBR Bindings Threshold Exceeded

Alarm Group: SBR

Description: The number of bindings threshold has been exceeded.

Severity:

- **Minor**: SBR active bindings threshold is greater than or equal to 80% of maximum binding capacity
- **Major**: SBR active bindings threshold is greater than or equal to 90% of maximum binding capacity
- **Critical**: SBR active bindings threshold is greater than or equal to 95% of maximum binding capacity

Instance: Policy Binding Region Place Association Name

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrActBindThreshNotify

Recovery:

1. This alarm indicates that the total number of subscribers that have at least one binding is nearing the tested maximum of the system. The alarm threshold percentages can be modified as desired by the network operator at the NOAMP using **Policy and Charging** > **Configuration** > **Alarm Settings**.

2. If a given alarm severity is unwanted, the alarm severity may be suppressed by checking the Suppress checkbox for that alarm severity.

3. Contact *My Oracle Support (MOS)* to discuss plans for system growth is this alarm continues to be asserted under normal operating conditions.

   Note: It is expected, but not guaranteed, that the system will continue to function beyond the tested maximum number of subscribers with bindings.

22729 - PCRF Not Configured

Alarm Group: PCA

Description: PCRF Not Configured

Severity: Major

Instance: Policy Binding Region Place Association Name

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: pdraPcrfNotConfiguredNotify

Recovery:

1. Check the NOAMP GUI at **Main Menu** > **Policy and Charging** > **Configuration** > **Policy DRA** for further PCRF configuration.
2. Check the event history logs in **Alarms & Events**.
3. If the problem persists, contact *My Oracle Support (MOS)*.

22730 - Policy and Charging Configuration Error

Alarm Group: PCA

Description: Policy and Charging message processing could not be successfully completed due to a configuration error.

Severity: Major

Instance: <ConfigurationError>

HA Score: Normal

OID: pdraPdraConfigErrorNotify

Auto Clear Seconds: 300

Recovery:

1. If there is an unconfigured PCRF, it means that the binding capable session initiation request was routed to a PCRF that is not configured in **Policy and Charging** > **Configuration** > **Policy DRA** > **PCRFs** at the site where the request was received. This indicates a mismatch between the PCRF's configuration and the routing configuration. If the PCRF is a valid choice for the request, configure the PCRF in **Policy and Charging** > **Configuration** > **Policy DRA** > **PCRFs**. If the PCRF is not valid for the request, correct the routing table or tables that included the PCRF.

Also see measurement *RxBindCapUnknownPcrf* in the *DSR Measurement Reference*.

2. If there is an unconfigured APN and if the APN string is valid, configure the APN at the NOAMP using the **Policy and Charging** > **Configuration** > **Access Point Names** screen. If the APN string is not valid, investigate the policy client to determine why it is sending policy session initiation requests using the invalid APN.

   Also see measurements *RxBindCapUnknownApn* and *RxBindDepUnknownApn* in the *DSR Measurement Reference*.

3. If there is a missing APN, investigate the policy client to determine why it is sending policy session initiation requests with no APN.

   Also see measurements *RxBindCapMissingApn* and *RxBindDepMissingApn* in the *DSR Measurement Reference*.

4. If there are no PCRFs configured, configure PCRFs at the SOAM GUI for the site using **Policy and Charging** > **Configuration** > **PCRFs**.

5. If there is an unconfigured OCS, it means that the binding independent session initiation request was routed to an OCS that is not configured in **Policy and Charging** > **Configuration** > **Online Charging DRA** > **OCSs**. This indicates a mismatch between the OCSs configuration and the routing configuration. If the OCS named in the alarm additional information is a valid choice for the request, configure the OCS at the SOAMP using **Policy and Charging** > **Configuration** > **Online Charging DRA** > **OCSs**. if the OCS is not valid for the request, correct the routing table or tables that included the OCS.

6. Contact *My Oracle Support (MOS)*

22731 - Policy and Charging Database Inconsistency

Alarm Group: PCA

Description: The Policy and Charging database inconsistency exists due to an internal data error or internal database table error.

Severity: Major

Instance: Policy DRA, Online Charging DRA

HA Score: Normal

Auto Clear Seconds: 60

OID: pdraPdraDbInconsistencyExistsNotify

Recovery:

1. Check the error history logs for the details of the data inconsistency.
2. If the problem persists, contact *My Oracle Support (MOS)*.

22732 - SBR Process CPU Utilization Threshold Exceeded

Alarm Group: SBR

Description: The SBR process on the indicated server is using higher than expected CPU resources.

Severity:

- **Minor**: SBR process CPU utilization threshold exceeds 60%
- **Major**: SBR process CPU utilization threshold exceeds 66%
- **Critical**: SBR process CPU utilization threshold exceeds 72%

Instance: Policy and Charging Mated Sites Place Association Name

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPSbrProcCpuThreshNotify

Recovery:

1. If this condition persists, it may be necessary to deploy more policy signaling capacity.
2. Contact *My Oracle Support (MOS)* for further assistance.

22733 - SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration

Alarm Group: SBR

Description: The SBR failed to free binding memory after PCRF Pooling binding migration.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: eagleXgDiameterPSBRPostMigrationMemFreeNotify

Recovery:

1. On systems upgraded from a release where Policy DRA was running, but that did not support PCRF Pooling, to a release that supports PCRF Pooling, binding data is migrated from the tables used by the old release to tables used by the new release. Once this migration process completes on a given binding policy SBR, a script is automatically executed to free memory for the old tables. If this script should fail for any reason to free the memory, this alarm is asserted.
2. If additional assistance is needed, contact *My Oracle Support (MOS)*.

22734 - Policy and Charging Unexpected Stack Event Version

Alarm Group: PCA

Description: A Policy and Charging server received a stack event with an unexpected down-version.

Severity: Major

Instance: N/A

HA Score: Normal

OID: pdraPdraUnexpectedSEDownVersionNotify

Auto Clear Seconds: 300

Recovery:

1. From the NOAMP GUI at **Policy and Charging** > **Maintenance** > **SBR Status**, find the Resource Domain Name to which the stack event was being sent.

2. Expand all Server Groups having that Resource Domain name to see which Server Group hosts the ComAgent Sub Resource.

3. The Server with Resource HA Role of "Active" is likely the server that has the old software (unless a switch-over has occurred since the alarm was asserted). In any case, one of the servers in the Server Group has old software. The software version running on each server can be viewed from **Administration** > **Upgrade**. The "Hostname" field is the same as the Server Name on the SBR Status screen

4. Find the server or servers running the old software and upgrade those servers to the current release and accept the upgrade.

5. If additional assistance is needed, contact *My Oracle Support (MOS)*.

22736 - SBR failed to free shared memory after a PCA function is disabled

Alarm Group: SBR

Description: SBR failed to free shared memory after a PCA function is disabled

Severity: Minor

HA Score: Normal

Instance: Policy DRA, Online Charging DRA

Auto Clear Seconds: 0 (zero)

OID: pdraPSBRPostPcaFunctionDisableMemFreeNotify

Recovery:

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

22737 - Configuration Database Not Synced

Alarm Group: PCA

Description: Configuration Database is not synced between the System OAM and Network OAMP

Severity: Minor

Instance: Site name of SOAM server which asserted this alarm

HA Score: Normal

OID: pdraPcaConfDbNotSyncedNotify

Auto Clear Seconds: 0

Recovery:

1. Make note of all **Status & Manage** > **Database Resote** operations (if any) at NOAMP or SOAM within a day of the occurrence of alarm.

2. Gather all configuration changes (Insert, Edit, or Delete) for PCRFs, Policy Clients, OCSs, CTFs via Security Log from the time the database restore was executed until the present. If there was no database restore performed, then start from the time the alarm was first asserted until the present.

3. If additional assistance is needed, contact *My Oracle Support (MOS)*.

Charging Proxy Application (CPA) Alarms and Events (22800-22849)

22805 - Message Decoding Failure

Event Type: CPA

Description: The CPA application could not decode a received Diameter message

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaMsgDecodeFailureNotify

Recovery:

1. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

   While parsing the message, the message content was inconsistent with the "Message Length" in the message header.

2. Contact *My Oracle Support (MOS)* for assistance.

22806 - Unknown Diameter Application Id

Event Type: CPA

Description: The CPA application received a Diameter message with an unexpected DSR application id. The DSR Relay Agent forwarded a Request message to the CPA application which contained an unrecognized Diameter Application ID in the header. A DSR Relay Agent application routing rule is mis-provisioned.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnknownAppIdNotify

Recovery:

1. Examine the DSR Relay Agent application routing rule for provisioning errors.

   The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.

2. Contact *My Oracle Support (MOS)* for assistance.

22807 - Unknown Command Code

Event Type: CPA

Description: The CPA application received a Diameter message other than an Accounting message. The Command Code received in the Diameter message is not an Accounting Message. A DSR Relay Agent application routing rule is mis-provisioned.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnknownCmdCodeNotify

Recovery:

1. Examine the DSR Relay Agent application routing rule for provisioning errors.

    The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.

2. Contact *My Oracle Support (MOS)* for assistance.

22808 - Session Not Found

Event Type: CPA

Description: The CPA queried the SBR and did not get a match for a Session Binding Record based on the session id. The CPA application expected a Session Binding Record but did not find one. This condition might indicate that the SBR has timed out the record and deleted it.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterCpaSessionNotFoundNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

22809 - Undelivered SBR Query

Event Type: CPA

Description: The ComAgent could not deliver the SBR query or no response was received from the SBR. This event is generated when the ComAgent times out an SBR query because it could not deliver it or no response was received from the far end.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUndeliveredSbrQueryNotify

Recovery:

1. Make sure the SBR MPs are not having networking trouble.
2. Contact *My Oracle Support (MOS)* for assistance.

22810 - Routing attempt failed due to internal resource exhaustion

Event Type: CPA

Description: An attempt to route a Diameter message through the DRL has failed due to resource exhaustion.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaRteFailResourceExhNotify

Recovery:

1. The MP may be experiencing local congestion.
2. Contact *My Oracle Support (MOS)* for assistance.

22811 - CPA Application Event Task Queue Utilization

Event Type: CPA

Description: The CPA Application's Event Queue Utilization is approaching its maximum capacity. The DSR Application's Event Queue (which processes SBR responses that are sent via ComAgent) is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: CPA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterCpaAppEventQueueUtilNotify

Recovery:

1. The alarm log should be examined using **Main Menu** > **Alarms & Events**.

If no additional congestion alarms are indicated, the CPA Event Task may be experiencing a problem preventing it from processing messages from its Event Queue.

2. If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22812 - Missing AVP

Event Type: CPA

Description: A received Diameter Accounting message does not contain the required Accounting Record Type or Accounting Record Number AVP.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaMissingAvpNotify

Recovery:

If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22813 - Received an error response to an SBR Query

Event Type: CPA

Description: CPA application received an error response in reply to an SBR query. An application specific error message was received in response to an SBR query.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterCpaSbrErrorRespNotify

Recovery:

If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22814 - HA Sub-Resource Unavailable

Event Type: CPA

Description: An HA Sub-Resource corresponding to a partition of the Session Binding Repository is unavailable. CPA has received a callback from ComAgent indicating that an HA sub-resource is unavailable.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaHASubResourceUnavailableNotify

Recovery:

If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22815 - Unexpected Session

Event Type: CPA

Description: A Session Binding Record was found when none was expected. CPA received an ACA-Start and found a Session Binding Record already exists.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnexpectedSessionNotify

Recovery:

If this problem persists, contact *My Oracle Support (MOS)* for assistance.

22816 - One or more cSBR Subresources Unavailable

Alarm Group: CPA

Description: One or more Charging SBR Subresources are unavailable.

Severity: Based on Subresources unavailable.

- Major - one or more (but not all) cSBR Subresources are unavailable.
- Critical - all cSBR Subresources are unavailable.

Instance: Site Id

HA Score: Normal

Auto Clear Seconds: N/A

OID: eagleXgDiameterCpaSbrSubresourceIsUnavailableNotify

Recovery:

1. Check the state of the SBR MPs.

   One or more Charging SBR subresources are unavailable. Make sure the SBR MPs are not having networking trouble.

2. Contact *My Oracle Support (MOS)* for assistance.

Tekelec Virtual Operating Environment, TVOE (24400-24499)

This section provides information and recovery procedures for the Tekelec Virtual Operation Environment (TVOE) alarms, ranging from 24400-24499.

24400 - TVOE libvirtd is down

Alarm Group: TVOE

Description: This alarm indicates that the libvirtd daemon is not running.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.1

Recovery:

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

24401 - TVOE libvirtd is hung

Alarm Group: TVOE

Description: This alarm indicates that we attempted to determine if the libvirtd daemon is not responding and it didn't respond.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.2

Recovery:

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

24402 - all TVOE libvirtd connections are in use

Alarm Group: TVOE

Description: This alarm indicates that all twenty connections to libvirtd are in use and more could be killed.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.3

Recovery:

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

Computer Aided Policy Making, CAPM (25000-25499)

This section provides information and recovery procedures for the Computer-Aided Policy Making (CAPM) feature (i.e., Diameter Mediation) alarms and events, ranging from 25000 - 25499, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

25000 - Rule Template failed to be updated

Event Type: CAPM

Description: The Rule Template failed to update because of syntax errors. The Additional Info of the Historical alarm includes the name of the Rule Template that failed to be updated.

When the alarm is caused by CAPM Rule Template which contains a syntax error, it may not be raised immediately after applying the template, but may occur when the first Rule has been provisioned and committed.

Severity: Minor

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterCapmUpdateFailedNotify

Recovery:

1. Check the CAPM Rule Template and verify that the left-hand side term of each condition contains a valid Linking-AVP or Select expression.

   A typical problem can be a non-existing expression, or syntax error of a custom-defined Select expression. If the CAPM Rule Template contains a syntax error, create a new Rule Template by copying and modifying the existing one, then deleting the old Rule Template.

2. Verify also that the recently provisioned data of the Rule Template does not contain a syntax error, i.e., the regular expressions are correct, the fields expecting numbers contain only numbers, etc.

25001 - Action failed within the Rule Template

Event Type: CAPM

Description: When a new Rule Template is created, a failure occurs when performing the action.

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmActionFailedNotify

Recovery:

Check the reasons the action failed. It may be a lack of system resources to perform an action, or the action may refer to a part of the message that is not available.

25002 - Stop Rule Template processing after action failure

Event Type: CAPM

Description: When Action Error Handling is set to 'immediately exit from the rule template' for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped.

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmExitRuleFailedNotify

Recovery:

No action required.

25003 - Exit Trigger point after action failure

Event Type: CAPM

Description: When Action Error Handling is set to 'immediately exit from the trigger point' for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped (subsequent templates within the trigger point are also skipped).

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmExitTriggerFailedNotify

Recovery:

No action required.

25004 - Script failed to load

Alarm Type: CAPM

Description: Script failed to load event

Severity: Minor

Instance: <script name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFCapmScriptLoadingFailureNotify

Recovery:

Check for syntax errors in the script

OAM Alarm Management (25500-25899)

This section provides information and recovery procedures related for alarms and events related to OAM Alarm Management, ranging from 25500 - 25899, that can occur on the system. All events have a severity of Info.

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

25500 - No DA-MP Leader Detected Alarm

Alarm Group: DIAM

Description: This alarm occurs when no active DA-MP leaders have been detected.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterNoDaMpLeaderDetectedNotify

Recovery:

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

25510 - Multiple DA-MP Leader Detected Alarm

Alarm Group: DIAM

Description: This alarm occurs when multiple active DA-MP leaders have been detected.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMultipleDaMpLeadersDetectedNotify

Recovery:

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

Platform (31000-32700)

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

31000 - S/W fault

Alarm Group: SW

Description: Program impaired by s/w fault

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSwFaultNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact *My Oracle Support (MOS)*.

31001 - S/W status

Alarm Group: SW

Description: Program status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSwStatusNotify

Recovery:

No action required.

31002 - Process watchdog failure

Alarm Group: SW

Description: Process watchdog timed out

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolProcWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact *My Oracle Support (MOS)*.

31003 - Tab thread watchdog failure

Alarm Group: SW

Description: Tab thread watchdog timed out

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolThreadWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact *My Oracle Support (MOS)*.

31100 - Database replication fault

Alarm Group: SW

Description: The Database replication process is impaired by a s/w fault

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbReplicationFaultNotify

Recovery:

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

31101 - Database replication to slave failure

Alarm Group: REPL

Description: Database replication to a slave Database has failed

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepToSlaveFailureNotify

Recovery:

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

31102 - Database replication from master failure

Alarm Group: REPL

Description: Database replication from a master Database has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepFromMasterFailureNotify

Recovery:

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

31103 - DB Replication update fault

Alarm Group: REPL

Description: Database replication process cannot apply update to DB

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepUpdateFaultNotify

Recovery:

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

31104 - DB Replication latency over threshold

Alarm Group: REPL

Description: Database replication latency has exceeded thresholds

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepLatencyNotify

Recovery:

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

31105 - Database merge fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeFaultNotify

Recovery:

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

31106 - Database merge to parent failure

Alarm Group: COLL

Description: Database merging to the parent Merge Node has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolDbMergeToParentFailureNotify

Recovery:

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

31107 - Database merge from child failure

Alarm Group: COLL

Description: Database merging from a child Source Node has failed

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeFromChildFailureNotify

Recovery:

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

31108 - Database merge latency over threshold

Alarm Group: COLL

Description: Database Merge latency has exceeded thresholds

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeLatencyNotify

Recovery:

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

31109 - Topology config error

Alarm Group: DB

Description: Topology is configured incorrectly

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolTopErrorNotify

Recovery:

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

31110 - Database audit fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbAuditFaultNotify

Recovery:

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

2. Contact *My Oracle Support (MOS)*.

31111 - Database merge audit in progress

Alarm Group: COLL

Description: Database Merge Audit between mate nodes in progress

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeAuditNotify

Recovery:

No action required.

31112 - Stateful db synchronization from mate server

Alarm Group: REPL

Description: Stateful database is not yet synchronized with mate database.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 30

OID: comcolDbRepUpLogTransTimeoutNotify

Recovery:

No action required. Contact *My Oracle Support (MOS)* if this occurs frequently.

31113 - DB replication manually disabled

Alarm Group: REPL

Description: DB Replication Manually Disabled

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolDbReplicationManuallyDisabledNotify

Recovery:

No action required.

31114 - DB replication over SOAP has failed

Alarm Group: REPL

Description: Database replication of configuration data via SOAP has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 3600

OID: comcolDbReplicationSoapFaultNotify

Recovery:

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

31115 - Database service fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbServiceFaultNotify

Recovery:

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

31116 - Excessive shared memory

Alarm Group: MEM

Description: The amount of shared memory consumed exceeds configured thresholds

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolExcessiveSharedMemoryConsumptionNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31117 - Low disk free

Alarm Group: DISK

Description: The amount of free disk is below configured thresholds

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolLowDiskFreeNotify

Recovery:

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

31118 - Database disk store fault

Alarm Group: DISK

Description: Writing the database to disk failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbDiskStoreFaultNotify

Recovery:

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

31119 - Database updatelog overrun

Alarm Group: DB

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpdateLogOverrunNotify

Recovery:

   Contact *My Oracle Support (MOS)*.

31120 - Database updatelog write fault

Alarm Group: DB

Description: A Database change cannot be stored in the updatelog

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpdateLogWriteFaultNotify

Recovery:

   Contact *My Oracle Support (MOS)*.

31121 - Low disk free early warning

Alarm Group: DISK

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolLowDiskFreeEarlyWarningNotify

Recovery:

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

31122 - Excessive shared memory early warning

Alarm Group: MEM

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

> Contact *My Oracle Support (MOS)*.

31123 - Database replication audit command complete

Alarm Group: REPL

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

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepAuditCmdCompleteNotify

Recovery:

> No action required.

31124 - ADIC error

Alarm Group: REPL

Description: An ADIC detected errors

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepAuditCmdErrNotify

Recovery:

    Contact *My Oracle Support (MOS)*.

31125 - Database durability degraded

Alarm Group: REPL

Description: Database durability has dropped below configured durability level

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbDurabilityDegradedNotify

Recovery:

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

31126 - Audit blocked

Alarm Group: REPL

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolAuditBlockedNotify

Recovery:

    Contact *My Oracle Support (MOS)*.

31127 - DB Replication Audit Complete

Alarm Group: REPL

Description: DB replication audit completed

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepAuditCompleteNotify

Recovery:

No action required.

31128 - ADIC Found Error

Alarm Group: REPL

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbADICErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31129 - ADIC Found Minor Issue

Alarm Group: REPL

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 14400

OID: comcolDbADICWarn

Recovery:

No action required.

31130 - Network health warning

Alarm Group: NET

Description: Network health issue detected

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolNetworkHealthWarningNotify

Recovery:

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

31131 - IDB Throttled for Extended Period

Alarm Group: DB

Description: IDB has one or more processes throttled for an extended period.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolOustedThrottleWarnNotify

Recovery:

1. Monitor for workload in excess of documented capacity.
2. Contact *My Oracle Support (MOS)* if this alarm persists.

31140 - Database perl fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbPerlFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31145 - Database SQL fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbSQLFaultNotify

Recovery:

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

31146 - DB mastership fault

Alarm Group: SW

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. Contact *My Oracle Support (MOS)*.

31147 - DB upsynclog overrun

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpSyncLogOverrunNotify

Recovery:

   Contact *My Oracle Support (MOS)*.

31148 - DB lock error detected

Alarm Group: DB

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbLockErrorNotify

Recovery:

   Contact *My Oracle Support (MOS)*.

31200 - Process management fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcMgmtFaultNotify

Recovery:

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

31201 - Process not running

Alarm Group: PROC

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcNotRunningNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31202 - Unkillable zombie process

Alarm Group: PROC

Description: A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcZombieProcessNotify

Recovery:

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

31206 - Process mgmt monitoring fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcMgmtMonFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31207 - Process resource monitoring fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcResourceMonFaultNotify

Recovery:

> Contact *My Oracle Support (MOS)*.

31208 - IP port server fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolPortServerFaultNotify

Recovery:

> Contact *My Oracle Support (MOS)*.

31209 - Hostname lookup failed

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHostLookupFailedNotify

Recovery:

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

31213 - Process scheduler fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcSchedulerFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31214 - Scheduled process fault

Alarm Group: PROC

Description: A scheduled process cannot be executed or abnormally terminated

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolScheduleProcessFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31215 - Process resources exceeded

Alarm Group: SW

Description: A process is consuming excessive system resources

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 14400

OID: comcolProcResourcesExceededFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31216 - SysMetric configuration error

Alarm Group: SW

Description: A SysMetric Configuration table contains invalid data

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSysMetricConfigErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31220 - HA configuration monitor fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaCfgMonitorFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31221 - HA alarm monitor fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAlarmMonitorFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31222 - HA not configured

Alarm Group: HA

Description: High availability is disabled due to system configuration

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaNotConfiguredNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31223 - HA Heartbeat transmit failure

Alarm Group: HA

Description: The high availability monitor failed to send heartbeat

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaHbTransmitFailureNotify

Recovery:

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

31224 - HA configuration error

Alarm Group: HA

Description: High availability configuration error

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID:comcolHaCfgErrorNotify

Recovery:

> Contact *My Oracle Support (MOS)*.

31225 - HA service start failure

Alarm Group: HA

Description: The high availability service failed to start

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaSvcStartFailureNotify

Recovery:

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

31226 - HA availability status degraded

Alarm Group: HA

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.

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

31227 - HA availability status failed

Alarm Group: HA

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAvailFailedNotify

Recovery:

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

31228 - HA standby offline

Alarm Group: HA

Description: High availability standby server is offline

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolHaStandbyOfflineNotify

Recovery:

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

31229 - HA score changed

Alarm Group: HA

Description: High availability health score changed

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaScoreChangeNotify

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolRecAlarmEvProcFaultNotify

Recovery:

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

31231 - Platform alarm agent fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolPlatAlarmAgentNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31232 - Late heartbeat warning

Alarm Group: HA

Description: High availability server has not received a message on specified path within the configured interval.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaLateHeartbeatWarningNotify

Recovery:

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

31233 - HA Path Down

Alarm Group: HA

Description: High availability path loss of connectivity

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaPathDownNotify

Recovery:

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

31234 - Untrusted Time Upon Initialization

Alarm Group: REPL

Description: Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolUtrustedTimeOnInitNotify

Recovery:

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

31235 - Untrusted Time After Initialization

Alarm Group: REPL

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0

OID: comcolUtrustedTimePostInitNotify

Recovery:

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

31236 - HA Link Down

Alarm Group: HA

Description: High availability TCP link is down.

Severity: Critical

Instance: Remote node being connected to plus the path identifier

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaLinkDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the specified path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.

2. If communication fails at any other time, look for network connectivity issues on the primary network and/or contact *My Oracle Support (MOS)*.

31240 - Measurements collection fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID:comcolMeasCollectorFaultNotify

Recovery:

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

31250 - RE port mapping fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolRePortMappingFaultNotify

Recovery:

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

31260 - SNMP Agent

Alarm Group: SW

Description: The SNMP agent (cmsnmpa) is impaired by a s/w fault

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbcomcolSnmpAgentNotify

Recovery:

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

31270 - Logging output

Alarm Group: SW

Description: Logging output set to Above Normal

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolLoggingOutputNotify

Recovery:

Extra diagnostic logs are being collected, potentially degrading system performance. Contact *My Oracle Support (MOS)*.

31280 - HA Active to Standby transition

Alarm Group: HA

Description: HA active to standby activity transition

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolActiveToStandbyTransNotify

Recovery:

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

31281 - HA Standby to Active transition

Alarm Group: HA

Description: HA standby to active activity transition

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolStandbyToActiveTransNotify

Recovery:

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

31282 - HA Management Fault

Alarm Group: HA

Description: The HA manager (cmha) is impaired by a software fault.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaMgmtFaultNotify

Recovery:

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

31283 - HA Server Offline

Alarm Group: HA

Description: High availability server is offline

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0

OID: comcolHaServerOfflineNotify

Recovery

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.

2. If communication fails at any other time, look for network connectivity issues and/or Contact *My Oracle Support (MOS)*.

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Group: HA

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRemoteHeartbeatWarningNotify

Recovery:

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

31285 - HA 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 Group: HA

Description: HA manager (cmha) status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaProcessStatusNotify

Recovery:

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

31291 - HA Election Status

Alarm Group: HA

Description: HA DC Election status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaElectionStatusNotify

Recovery:

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

31292 - HA Policy Status

Alarm Group: HA

Description: HA Policy plan status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaPolicyStatusNotify

Recovery:

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

31293 - HA Resource Link Status

Alarm Group: HA

Description: HA ResourceAgent Link status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaLinkStatusNotify

Recovery:

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

31294 - HA Resource Status

Alarm Group: HA

Description: HA Resource registration status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaResourceStatusNotify

Recovery:

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

31295 - HA Action Status

Alarm Group: HA

Description: HA Resource action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

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 Group: HA

Description: HA Monitor action status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaMonitorStatusNotify

Recovery:

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 Group: HA

Description: HA Resource Agent Info

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaInfoNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.

2. Otherwise, contact *My Oracle Support (MOS)*.

31298 - HA Resource Agent Detail

Alarm Group: HA

Description: Resource Agent application detailed information

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaDetailNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.

2. Otherwise, contact *My Oracle Support (MOS)*.

31299 - HA Notification Status

Alarm Group: HA

Description: HA Notification status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaNotificationNotify

Recovery:

No action required.

31300 - HA Control Status

Alarm Group: HA

Description: HA Control action status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaControlNotify

Recovery:

No action required.

32100 - Breaker Panel Feed Unavailable

Alarm Group: PLAT

Description: Breaker Panel Breaker Unavailable

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlFeedUnavailable

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Group: PLAT

Description: Breaker Panel Breaker Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlBreakerFailure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

Alarm Group: PLAT

Description: Breaker Panel Monitoring Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlMntFailure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32103 - Power Feed Unavailable

Alarm Group: PLAT

Description: Power Feed Unavailable

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerFeedUnavail

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Group: PLAT

Description: Power Supply 1 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply1Failure

Recovery

> Contact *My Oracle Support (MOS)* to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Group: PLAT

Description: Power Supply 2 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply2Failure

Recovery

> Contact *My Oracle Support (MOS)* to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group: PLAT

Description: Power Supply 3 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply3Failure

Recovery

> Contact *My Oracle Support (MOS)* to request hardware replacement.

32107 - Raid Feed Unavailable

Alarm Group: PLAT

Description: Raid Feed Unavailable

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidFeedUnavailable

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Group: PLAT

Description: Raid Power 1 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidPower1Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Group: PLAT

Description: Raid Power 2 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidPower2Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Group: PLAT

Description: Raid Power 3 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidPower3Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32111 - Device Failure

Alarm Group: PLAT

Description: Device Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceFailure

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

32112 - Device Interface Failure

Alarm Group: PLAT

Description: Device Interface Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceIfFailure

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

32113 - Uncorrectable ECC memory error

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdEccUncorrectableError

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

32114 - SNMP get failure

Alarm Group: PLAT

Description: The server failed to receive SNMP information from the switch.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSNMPGetFailure

Recovery:

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

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPDaemonNotSynchronizedFailure

Recovery:

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

32116 - TPD Server's Time Has Gone Backwards

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPTimeGoneBackwards

Recovery:

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

32117 - TPD NTP Offset Check Failure

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ntpOffsetCheckFailure

Recovery:

Contact *My Oracle Support (MOS)*.

32300 – Server fan failure

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdFanError

Recovery

Contact *My Oracle Support (MOS)*.

32301 - Server internal disk error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdIntDiskError

Recovery

Contact *My Oracle Support (MOS)*.

32302 – Server RAID disk error

Alarm Group: PLAT

Description: This alarm indicates that the offboard storage server had a problem with its hardware disks.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidDiskError

Recovery

Contact *My Oracle Support (MOS)*.

32303 - Server Platform error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPlatformError

Recovery

Contact *My Oracle Support (MOS)* and provide the system health check output.

32304 - Server file system error

Alarm Group: PLAT

Description: This alarm indicates unsuccessful writing to at least one of the server's file systems.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdFileSystemError

Recovery

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

32305 - Server Platform process error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPlatProcessError

Recovery

Contact *My Oracle Support (MOS)*.

32306 – Server RAM shortage error

Alarm Group: PLAT

Not Implemented.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRamShortageError

Contact *My Oracle Support (MOS)*.

32307 - Server swap space shortage failure

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSwapSpaceShortageError

Recovery

Contact *My Oracle Support (MOS)*.

32308 - Server provisioning network error

Alarm Group: PLAT

Description: This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdProvNetworkError

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)*.

32309 - Eagle Network A Error

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdEagleNetworkAError

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32310 - Eagle Network B Error

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdEagleNetworkBError

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32311 - Sync Network Error

Alarm Group: PLAT

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSyncNetworkError

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32312 - Server disk space shortage error

Alarm Group: PLAT

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

- A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system.

- More than 90% of the total number of available files have been allocated on the file system.

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskSpaceShortageError

Recovery

Contact *My Oracle Support (MOS)*.

32313 - Server default route network error

Alarm Group: PLAT

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

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDefaultRouteNetworkError

Recovery

Contact *My Oracle Support (MOS)*.

32314 - Server temperature error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdServerTemperatureError

Recovery

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

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

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

32315 - Server mainboard voltage error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdServerMainboardVoltageError

Recovery

> Contact *My Oracle Support (MOS)*.

32316 – Server power feed error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerFeedError

Recovery

1. Verify that all the server power feed cables to the server that is reporting the error are securely connected.
2. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.

3. Follow the power feed to its connection on the power source. Ensure that the power source is ON and that the power feed is properly secured.
4. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.

5. If the power source is functioning properly and the wires are all secure, have an electrician check the voltage on the power feed.

6. Check to see if the alarm has cleared

   • If the alarm has been cleared, the problem is resolved.
   • If the alarm has not been cleared, continue with the next step.

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

32317 - Server disk health test error

Alarm Group: PLAT

Description: Either the hard drive has failed or failure is imminent.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskHealthError

Recovery

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

32318 - Server disk unavailable error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskUnavailableError

Recovery

Contact *My Oracle Support (MOS)*.

32319 – Device error

Alarm Group: PLAT

This alarm indicates that the offboard storage server had a problem with its disk volume filling up.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceError

Recovery

Contact the *My Oracle Support (MOS)*.

32320 – Device interface error

Alarm Group: PLAT

Description: This alarm indicates that the IP bond is either not configured or down.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceIfError

Recovery

Contact *My Oracle Support (MOS)*.

32321 – Correctable ECC memory error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdEccCorrectableError

Recovery

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

32322 – Power Supply A error

Alarm Group: PLAT

Description: This alarm indicates that power supply 1 (feed A) has failed.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply1Error

Recovery

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

32323 – Power Supply B error

Alarm Group: PLAT

Description: This alarm indicates that power supply 2 (feed B) has failed.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply2Error

Recovery

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

32324 – Breaker panel feed error

Alarm Group: PLAT

Description: This alarm indicates that the server is not receiving information from the breaker panel relays.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlFeedError

Recovery

1. Verify that the same alarm is displayed by multiple servers:

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

2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.

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

32325 – Breaker panel breaker error

Alarm Group: PLAT

Description: This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see *Figure 16: Breaker Panel LEDs*) identify whether the fault occurred on the input power or the output power, as follows:

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

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

- A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.
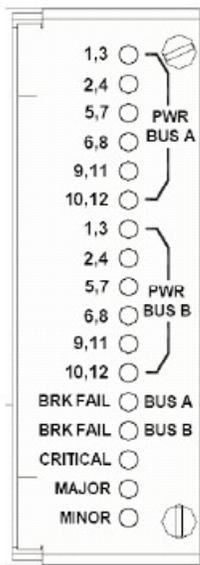
Figure 16: Breaker Panel LEDs

Description: This alarm indicates that a power fault has been identified by the breaker panel.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

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.
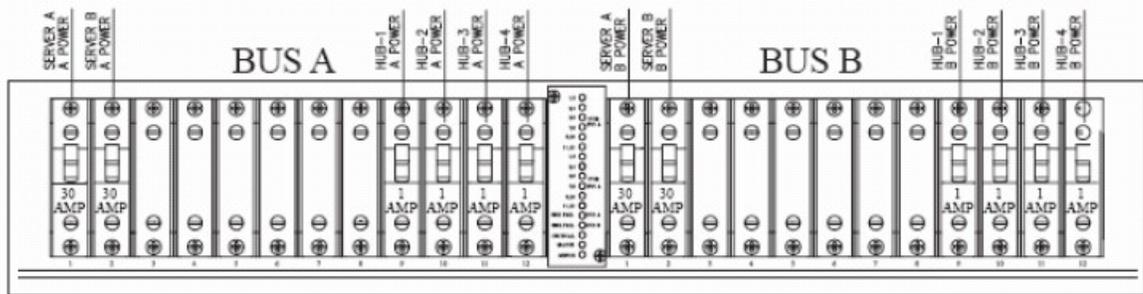
Figure 17: Breaker Panel Setting

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

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

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

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

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

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

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

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

32326 – Breaker panel monitoring error

Alarm Group: PLAT

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

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

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

until the Breaker Panel Monitoring Error has been corrected.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlMntError

Recovery

1. Verify that the same alarm is displayed by multiple servers:

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

2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).

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

32327 – Server HA Keepalive error

Alarm Group: PLAT

Description: This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHaKeepaliveError

Recovery

1. Determine if the mate server is currently down and bring it up if possible.

2. Determine if the keepalive interface is down.

3. Determine if heartbeart is running (service TKLCha status).

   Note: This step may require command line ability.

4. Contact *My Oracle Support (MOS)*.

32328 – DRBD is unavailable

Alarm Group: PLAT

Description: This alarm indicates that DRBD is not functioning properly on the local server. The DRBD state (disk state, node state, and/or connection state) indicates a problem.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdUnavailable

Recovery

Contact *My Oracle Support (MOS)*.

32329 – DRBD is not replicating

Alarm Group: PLAT

Description: This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdNotReplicating

Recovery

Contact *My Oracle Support (MOS)*.

32330 – DRBD peer problem

Alarm Group: PLAT

Description: This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdPeerProblem

Recovery

Contact the *My Oracle Support (MOS)*.

32331 – HP disk problem

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHpDiskProblem

Recovery

Contact *My Oracle Support (MOS)*.

32332 – HP Smart Array controller problem

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHpDiskCtrlrProblem

Recovery

Contact *My Oracle Support (MOS)*.

32333 – HP hpacucliStatus utility problem

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHPACUCLIProblem

Recovery

Contact *My Oracle Support (MOS)*.

32334 - Multipath device access link problem

Alarm Group: PLAT

Description: One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMpathDeviceProblem

Recovery:

32335 - Switch link down error

Alarm Group: PLAT

Description: The link is down.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSwitchLinkDownError

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 Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHalfOpenSockLimit

Recovery

Contact *My Oracle Support (MOS)*.

32339 - Max pid limit

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMaxPidLimit

Recovery:

Contact *My Oracle Support (MOS)*.

32340 - Server NTP Daemon Lost Synchronization For Extended Time

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPDaemonNotSynchronizedError

Recovery:

1. Verify NTP settings and that NTP sources can be reached.

2. Contact *My Oracle Support (MOS)*.

32341 - Server NTP Daemon Never Synchronized Error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPDaemonNeverSynchronized

Recovery:

1. Verify NTP settings and that NTP sources can be reached.

2. Contact *My Oracle Support (MOS)*.

32342 - NTP Offset Check Error

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ntpOffsetCheckError

Recovery:

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

2. Contact *My Oracle Support (MOS)*.

32343 - RAID disk problem

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskProblem

Recovery:

Contact *My Oracle Support (MOS)*.

32344 - RAID controller problem

Alarm Group: PLAT

Description: This alarms indicates that RAID controller needs intervention.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskCtrlrProblem

Recovery:

Contact *My Oracle Support (MOS)*.

32345 - Server Upgrade snapshot(s) invalid

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdUpgradeSnapshotInvalid

Recovery:

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

32346 - Server Hardware Problem

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdOEMHardware

Recovery:

Contact *My Oracle Support (MOS)*

32347 - Oracle hwmgmtcliStatus Problem

Alarm Group: PLAT

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHWMGMTCLIProblem

Recovery:

Contact *My Oracle Support (MOS)*

32500 – Server disk space shortage warning

Alarm Group: PLAT

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

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskSpaceShortageWarning

Recovery

Contact *My Oracle Support (MOS)*.

32501 – Server application process error

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdApplicationProcessError

Recovery

Contact *My Oracle Support (MOS)*.

32502 – Server hardware configuration error

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHardwareConfigError

Recovery

Contact *My Oracle Support (MOS)*.

32503 – Server RAM shortage warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRamShortageWarning

Recovery

Contact the *My Oracle Support (MOS)*.

32504 – Software Configuration Error

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSoftwareConfigError

Recovery

Contact *My Oracle Support (MOS)*.

32505 – Server swap space shortage warning

Alarm Group: PLAT

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

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSwapSpaceShortageWarning

Recovery

Contact *My Oracle Support (MOS)*.

32506 – Server default router not defined

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDefaultRouteNotDefined

Recovery

Contact *My Oracle Support (MOS)*.

32507 – Server temperature warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdServerTemperatureWarning

Recovery

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

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

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

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

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

32508 – Server core file detected

Alarm Group: PLAT

Description: This alarm indicates that an application process has failed and debug information is available.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdServerCoreFileDetected

Recovery

Contact *My Oracle Support (MOS)*.

32509 – Server NTP Daemon not synchronized

Alarm Group: PLAT

Description: This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPDeamonNotSynchronizedWarning

Recovery

Contact *My Oracle Support (MOS)*.

32510 – CMOS battery voltage low

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdCMOSBatteryVoltageLow

Recovery

    Contact *My Oracle Support (MOS)*.

32511 – Server disk self test warning

Alarm Group: PLAT

Description: A non-fatal disk issue (such as a sector cannot be read) exists.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSmartTestWarn

Recovery

    Contact *My Oracle Support (MOS)*.

32512 – Device warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceWarn

Recovery

    Contact *My Oracle Support (MOS)*.

32513 – Device interface warning

Alarm Group: PLAT

Description: This alarm can be generated by either an SNMP trap or an IP bond error.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceIfWarn

Recovery

Contact *My Oracle Support (MOS)*.

32514 – Server reboot watchdog initiated

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdWatchdogReboot

Recovery

Contact *My Oracle Support (MOS)*.

32515 – Server HA failover inhibited

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHaInhibited

Recovery

Contact *My Oracle Support (MOS)*.

32516 – Server HA Active to Standby transition

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHaActiveToStandbyTrans

Recovery

Contact *My Oracle Support (MOS)*.

32517 – Server HA Standby to Active transition

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHaStandbyToActiveTrans

Recovery

Contact *My Oracle Support (MOS)*.

32518 – Platform Health Check failure

Alarm Group: PLAT

Description: This alarm is used to indicate a configuration error.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHealthCheckFailed

Recovery

Contact *My Oracle Support (MOS)*.

32519 – NTP Offset Check failure

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ntpOffsetCheckWarning

Recovery

Contact *My Oracle Support (MOS)*.

32520 – NTP Stratum Check failure

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ntpStratumCheckFailed

Recovery

Contact *My Oracle Support (MOS)*.

32521 – SAS Presence Sensor Missing

Alarm Group: PLAT

Description: This alarm indicates that the T1200 server drive sensor is not working.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: sasPresenceSensorMissing

Recovery

> Contact *My Oracle Support (MOS)* to get a replacement server.

32522 – SAS Drive Missing

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: sasDriveMissing

Recovery

> Contact *My Oracle Support (MOS)* to determine whether the issue is with a failed drive or failed configuration.

32523 – DRBD failover busy

Alarm Group: PLAT

Description: This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdFailoverBusy

Recovery

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

32524 – HP disk resync

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHpDiskResync

Recovery

> Contact *My Oracle Support (MOS)*.

32525 – Telco Fan Warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdTelcoFanWarning

Recovery

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

32526 – Telco Temperature Warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdTelcoTemperatureWarning

Recovery

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

32527 – Telco Power Supply Warning

Alarm Group: PLAT

Description: This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdTelcoPowerSupplyWarning

Recovery

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

32528 – Invalid BIOS value

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdInvalidBiosValue

Recovery

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

32529 – Server Kernel Dump File Detected

Alarm Group: PLAT

Description: This alarm indicates that the kernel has crashed and debug information is available.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdServerKernelDumpFileDetected

Recovery

Contact *My Oracle Support (MOS)*.

32530 – Server Upgrade Fail Detected

Alarm Group: PLAT

Description: This alarm indicates that a TPD upgrade has failed.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: pdServerUpgradeFailed

Recovery

Contact *My Oracle Support (MOS)*.

32531 – Half Open Socket Warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHalfOpenSocketWarning

Recovery

Contact *My Oracle Support (MOS)*.

32532 – Server Upgrade Pending Accept/Reject

Alarm Group: PLAT

Description: This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdServerUpgradePendingAccept

Recovery

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

32533 - Max pid warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdMaxPidWarning

Recovery:

Contact *My Oracle Support (MOS)*.

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

Alarm Group: PLAT

Description: This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdNTPSourceIsBad

Recovery:

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

32535 - RAID disk resync

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDiskResync

Recovery:

If this alarm persists for several hours (depending on a load of a server rebuild of array can take multiple hours to finish), contact *My Oracle Support (MOS)*.

32536 - Server Upgrade snapshot(s) warning

Alarm Group: PLAT

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdUpgradeSnapshotWarning

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. Contact *My Oracle Support (MOS)*

32700 - Telco Switch Notification

Alarm Group: PLAT

Description: Telco Switch Notification

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 30

OID: tpdTelcoSwitchNotification

Recovery

Contact *My Oracle Support (MOS)*.

DM-IWF (33000-33024)

This section provides information and recovery procedures for DM-IWF) alarms and events, ranging from 33000 to 33024, and lists the type of alarms and events that can occur on the system.

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

33000 - MAP-to-Diameter Service Registration Failure on DA-MP

Alarm Group: DIWF

Description: DM-IWF application was unable to register for MAP-to-Diameter transaction service. No MAP-to-Diameter transactions can be routed to this DA-MP.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppComagentProviderRegistrationFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

33001 - Diameter-to-MAP Service Registration Failure on DA-MP

Alarm Group: DIWF

Description: DM-IWF application was unable to register for Diameter-to-MAP transaction service. Diameter-to-MAP transactions cannot be serviced by this DA-MP.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppComagentUserRegistrationFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for assistance.

33002 - DM-IWF DA-MP not associated with a Place

Alarm Group: DIWF

Description: DM-IWF DA-MP server is not associated with an AppWorks Place

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppServerPlaceFailureNotify

Recovery:

1. If the Server is not associated with an AppWorks place, Admin Disable DM-IWF on the DA-MP Server, add the Server to an appropriate AppWorks Place, and then Admin Enable DM-IWF on the DA-MP Server.
2. Contact *My Oracle Support (MOS)* for further assistance.

33003 - Insufficient memory for DM-IWF

Alarm Group:

Description: DA-MP does not have sufficient memory to support DM-IWF

Severity: Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppInsufficientMemoryFailureNotify

Recovery:

1. If the VM:Database DA-MP profile is applied to the DA-MP (**Main Menu** > **Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**), verify that the DA-MP has at least 24GB of physical memory.

2. If the G6:Database or G6:Session DA-MP profile is applied to the DA-MP (**Main Menu** > **Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**), verify that the DA-MP has at least 48GB of physical memory.

3. If the G7:Database, G8:Database, G7:Session or G8:Session DA-MP profile is applied to the DA-MP (**Main Menu** > **Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**), verify that the DA-MP has at least 64GB of physical memory.

4. If the DA-MP does not have sufficient physical memory to support a profile, contact *My Oracle Support (MOS)* for further assistance on how to upgrade memory.

33004 - DM-IWF Transaction Response Queue Utilization

Alarm Group: DIWF

Description: The DM-IWF Transaction Response Queue Utilization is approaching its maximum engineered capacity.

Severity: Minor, Major, Critical

Instance: RxDmiwfTranRspMsgQueue, DM-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppTransactionResponseQueueUtilizationNotify

Recovery:

1. This alarm should not normally occur when no other congestion alarms are asserted. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its transaction response queue. Examine the Alarm log in **Alarms & Events.**

2. Contact *My Oracle Support (MOS)* for assistance.

33005 - DM-IWF PTR Pool Utilization

Alarm Group: DIWF

Description: The DM-IWF PTR Pool Utilization is approaching its maximum engineered capacity. DM-IWF allocates a pending transaction record (PTR) for every pending Diameter-to-MAP and MAP-to-Diameter transaction. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppPTRPoolUtilizationNotify

Recovery:

1. Examine the Alarm log in **Alarms & Events** a evaluate whether the DSR Application Task might be experiencing a problem processing the messages. The rate of messages being processed by DM-IWF can be monitored from the from **Status & Manage > KPIs** page
2. If one or more DA-MPs in a server site have failed, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DA-MP server status can be monitored from the **Status & Manage > Server**.
3. 3. If one or more DM-IWF instances configured in a server site are unable to provide service, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DM-IWF application admin state can be monitored from Main Menu > Diameter > Maintenance > Applications. DM-IWF service provider status can be monitored from **Main Menu > Communication Agent > Maintenance > Routed Services Status**
4. If the problem persists, contact *My Oracle Support (MOS)*.

33006 - MD-IWF Service Congestion

Event Group: DIWF

Description: DM-IWF could not forward a Request to MD-IWF due to MD-IWF Service Congestion

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfServiceCongestedNotify

Recovery:

1. The number of SS7-MPs that act as providers for the MAP Routed Service might be insufficient to service the offered ingress load. MAP Routed Service ("MDIWFSvc") provider status can be monitored from **Main Menu > Communication Agent > Maintenance > Routed Services Status**.
2. If the problem occurs frequently, contact *My Oracle Support (MOS)*.

33007 - MD-IWF Error

Event Group: DIWF

Description: DM-IWF received notification indicating ComAgent Error/Timeout or MD-IWF Application generated Failure Response.

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfErrorNotify

Recovery:

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

33008 - DM-IWF maximum pending transactions allowed exceeded

Event Group: DIWF

Description: DM-IWF rejected either a Diameter-to-MAP or MAP-to-Diameter transaction because it was unable to allocation a pending transaction record (PTR) for the transaction. DM-IWF allocates a PTR for every pending Diameter-to-MAP and MAP-to-Diameter transaction. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfMaxPendTransactionsAllowedExceededNotify

Recovery:

1. Examine the Alarm log in **Alarms & Events** a evaluate whether the DSR Application Task might be experiencing a problem processing the messages. The rate of messages being processed by DM-IWF can be monitored from the from **Status & Manage > KPIs** page
2. If one or more DA-MPs in a server site have failed, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DA-MP server status can be monitored from the **Status & Manage > Server**.
3. 3. If one or more DM-IWF instances configured in a server site are unable to provide service, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DM-IWF application admin state can be monitored from Main Menu > Diameter > Maintenance > Applications. DM-IWF service provider status can be monitored from **Main Menu > Communication Agent > Maintenance > Routed Services Status**
4. If the problem persists, contact *My Oracle Support (MOS)*.

33009 - DM-IWF unexpected Answer response received from a SS7-MP

Event Group: DIWF

Description: No pending transaction was found for the Answer response received from SS7-MP. When a Request message is forwarded to an SS7-MP, DM-IWF creates a pending transaction record (PTR). The PTR is abandoned if an Answer response is not received in a timely fashion.

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfUnexpectedAnswerRspReceivedFromSS7MPNotify

Recovery:

1. If this event is occurring frequently, the MAP Response Timeout may be set too low. The MAP Response Timeout value can be reviewed via **Main Menu -> MAP-Diameter IWF -> Configuration -> MD-IWF Options** screen.

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

33010 - MD-IWF ComAgent Connection exhausted

Event Group: DIWF

Description: DM-IWF failed to receive a Diameter Answer in response to a Diameter Request that was forwarded to MD-IWF Routed Service, in a timely fashion

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfMapComAgentConnectionExhaustedNotify

Recovery:

1. If this event is occurring frequently, the MAP Response Timeout may be set too low. The MAP Response Timeout value can be reviewed via **Main Menu -> MAP-Diameter IWF -> Configuration -> MD-IWF Options** screen.

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

33011 - DM-IWF Answer Timeout

Event Group: DIWF

Description: DM-IWF failed to receive a Diameter Answer in response to a Diameter Request that was forwarded to MD-IWF Routed Service, within the DM-IWF Pending Answer Timer expiration.

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAnswerTimeoutNotify

Recovery:

1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. It's possible that the MAP Origination Transaction Timer value is set too low. The MAP Origination Transaction Timer value setting can be viewed via the following GUI screen: **Main Menu** > **MAP Interworking** > **Configuration** > **Options (MD-IWF tab)**.

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

33012 - DM-IWF encode decode error

Event Group: DIWF

Description: The decoder has reported an error causing the Request to be discarded.

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfDecodeErrorNotify

Recovery:

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

33013 - DRL queue exhaustion

Event Group: DIWF

Description: DM-IWF failed to forward a Diameter message to DRL due to DRL queue exhaustion

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDrlQueueExhaustionNotify

Recovery:

Note: This alarm should not occur unless the MP is experiencing local congestion as indicated by Alarms 22000 - Local MP Congestion, 22201 - Ingress Message Rate, 22204 - Request Message Queue Utilization, and 22205 - Answer Message Queue Utilization. Refer to the *DSR Alarms and KPIs Reference* for details about these alarms.

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

33014 - Incompatible DA-MP Profile for DM-IWF

Alarm Group: DIWF

Description: DA-MP has been assigned a profile that is incompatible with DM-IWF

Severity: Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDmiwfAppIncompatibleProfileFailureNotify

Recovery:

1. If the DA-MP has been assigned a DA-MP profile (**Main Menu** > **Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**) other than those listed below, apply a compatible profile and restart DSR (**Main Menu** > **Status & Manage** > **Server** > **Restart**.

   - G6:Database
   - G7:Database
   - G8:Database
   - VM:Database
   - G6:Session
   - G7:Session
   - G8:Session

2. If the DA-MP has been assigned a compatible profile and the problem persists, contact Customer Care Center for assistance.

3. If needed, contact *My Oracle Support (MOS)* for further assistance.

33015 - DM-IWF Diameter message size exceeded maximum supported size

Event Group: DIWF

Description: DM-IWF failed to forward the Diameter message to SS7-MP because the message size exceeds supported maximum message size

Severity: Info

Instance: <DAMPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDmiwfMaxDiameterMsgSizeExceededNotify

Recovery:

Occurrence of this event indicates that diameter message received has size that exceeds maximum diameter message size supported by MAP-Diameter Interworking function and therefore be handled as "Internal Processing Error". Source of these requests can be tracked using "Origin Host", "Application Id" and "Command Code".

MD-IWF (33050-33099)

This section provides information and recovery procedures for MD-IWF alarms and events, ranging from 33050 to 33099, and lists the type of alarms and events that can occur on the system.

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

33050 - MD-IWF Ingress Message Rate

Alarm Group: MIWF

Description: The ingress message rate for the MD-IWF Application is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfIngressMsgRateNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. Contact *My Oracle Support (MOS)* for further assistance.

33051 - MD-IWF Application Degraded or Unavailable

Alarm Group: MIWF

Description: MD-IWF Application operational status is Degraded or Unavailable.

Severity: Major, Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfApplDegradedOrUnavailableNotify

Recovery:

1. An MD-IWF Application operational status becomes Degraded when either the Admin State is set to disabled with the forced shutdown option or the Admin State is set to disabled with the graceful shutdown option and the graceful shutdown timer expires.
2. The MD-IWF Application can also become Degraded when it reaches Congestion Level 1, 2, or 3 if enabled.

   Note: This alarm will NOT be raised when the MD-IWF application is shutting down gracefully or application is in Disabled state. Only the MD-IWF Application operational status will be changed to Unavailable.

3. An MD-IWF Application operational status becomes Unavailable when either the Admin State is set to disabled with the forced shutdown option or the Admin State is set to disabled with the graceful shutdown option and the graceful shutdown timer expires.

4. The MD-IWF Application can also become Unavailable when it is isolated from the SS7 network.

   Note: This alarm will NOT be raised when the MD-IWF application is shutting down gracefully or application is in Disabled state. Only the MD-IWF Application operational status will be changed to Unavailable.

5. Monitor the MD-IWF Application status can be monitored from **Main Menu** > **Diameter** > **Maintenance** > **Applications**. Verify the admin state is set as expected.

6. Check the event history logs for additional events or alarms from this SS7-MP server.

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

33052 - MD-IWF Notified that DM-IWF Service Status is Down

Alarm Group: MIWF

Description: The MD-IWF is notified via ComAgent that the rolled-up DM-IWF Service Status is Down.

Severity: Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfUserSvcDownNotify

Recovery:

1. Investigate the status of all DA-MP servers. As this status is a rolled-up status, it indicates that no DA-MP servers are able to be a provider of the DM-IWF ComAgent Routed Service.

2. Contact *My Oracle Support (MOS)* for further assistance.

33053 - MD-IWF DiamTrans Task Queue Utilization

Alarm Group: MIWF

Description: The MD-IWF Application DiamTrans Task Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxMdIwfDiamTransMsgQueue (TaskID), MD-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamTransQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.
2. If no additional congestion alarms are asserted, the MD-IWF Application Task may be experiencing a problem preventing it from processing messages from its DiamTrans Task Queue. Examine the alarm log from **Main Menu** > **Alarms & Events**.
3. Contact *My Oracle Support (MOS)* for further assistance.

33054 - MD-IWF MapTrans Task Queue Utilization

Alarm Group: MIWF

Description: The MD-IWF Application MapTrans Task Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxMdIwfMapTransMsgQueue (TaskId), MD-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfMapTransQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.
2. If no additional congestion alarms are asserted, the MD-IWF Application Task may be experiencing a problem preventing it from processing messages from its DiamTrans Task Queue. Examine the alarm log from **Main Menu** > **Alarms & Events**.
3. Contact *My Oracle Support (MOS)* for further assistance.

33055 - MD-IWF DAMPInterface Task Queue Utilization

Alarm Group: MIWF

Description: The MD-IWF Application DAMPInterface Task Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxMdIwfDampInterfaceMsgQueue, MD-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDampInterfaceQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.

2. If no additional congestion alarms are asserted, the MD-IWF Application Task may be experiencing a problem preventing it from processing messages from its DAMPInterface Task Queue. Examine the alarm log from **Main Menu** > **Alarms & Events**.

3. Contact *My Oracle Support (MOS)* for further assistance.

33056 - MD-IWF ComAgent Provider Registration Failure on SS7-MP

Alarm Group: MIWF

Description: MD-IWF Application was unable to register with ComAgent as a provider of the MDIWFSvc service. No Diameter-to-MAP transactions can be routed to this SS7-MP.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfComAgentProviderRegisFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

33057 - MD-IWF ComAgent User Registration Failure on SS7-MP

Alarm Group: MIWF

Description: MD-IWF application was unable to register with ComAgent as a user of the DMIWFSvc service. MAP-to-Diameter transactions cannot be processed by this SS7-MP.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfComAgentUserRegisFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* for further assistance.

33058 - MD-IWF DiamToMap PTR Utilization

Alarm Group: MIWF

Description: The MD-IWF Application DiamToMap PTR Utilization is approaching its maximum engineered capacity.

Severity: Minor, Major, Critical

Instance: EvMdIwfDiam2MapPtrUtil, MD-IWF

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamToMapPtrUtilNotify

Recovery:

1. A DiamToMap PTR is allocated for every pending Diameter-to-Map transaction. The PTR size is engineered based on an average transaction holding size. If the PTRs becomes depleted, no new transactions can be processed by the MD-IWF application.
2. PTR exhaustion is most likely caused by long delays in the Diameter or SS7 networks. PTR exhaustion problems can be reduced/eliminated by reducing the MAP timer values.
3. View the current MAP timers from **Main Menu** > **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.
4. Contact *My Oracle Support (MOS)* for further assistance.

33059 - MD-IWF MapToDiam PTR Utilization

Alarm Group: MIWF

Description: MD-IWF Application MapToDiam PTR Utilization is approaching its maximum engineered capacity.

Severity: Minor, Major, Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfMapToDiamPtrUtilNotify

Recovery:

1. A MapToDiam PTR is allocated for every pending MAP-to-Diameter transaction. The size of the PTR size is engineered based on an average transaction holding size. If the PTRs become depleted, no new transactions can be processed by the MD-IWF application.
2. Determine if there are long delays in the Diameter or SS7 networks. PTR pool exhaustion can be reduced or eliminated by reducing the MAP timer values.
3. The current MAP timers can be viewed in the GUI at **Main Menu** > **MAP Interworking** > **Configuration** > **MD-IWF Options**.
4. Contact *My Oracle Support (MOS)* for further assistance.

33060 - SS7-MP Profile Not Assigned

Alarm Group: MIWF

Description: An SS7-MP configuration profile has not been assigned to this SS7-MP

Severity: Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterSs7MpProfileNotAssignedNotify

Recovery:

1. If the SS7-MP has been assigned an MP Profile from an SO GUI **Main Menu** > **Diameter Common** > **MPs** > **Profile Assignment** other MD-IWF, apply a compatible profile and restart the mapiwf process from **Main Menu** > **Status & Manage** > **Server**.
2. If the SS7-MP has been assigned a compatible profile already, contact *My Oracle Support (MOS)* for further assistance.

33062 - Insufficient Memory for MD-IWF

Alarm Group: MIWF

Description: SS7-MP does not have sufficient memory to support MD-IWF

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfInsufficientMemoryForMdiwfNotify

Recovery:

1. If MD-IWF was mistakenly activated, deactivate MD-IWF.
2. If the SS7-MP does not have sufficient physical memory, upgrade the memory.
3. Contact *My Oracle Support (MOS)* for further assistance.

33063 - MD-IWF SS7-MP not associated with a Place

Alarm Group: MIWF

Description: SS7-MP does not have sufficient memory to support MD-IWF

Severity: Critical

Instance: Default

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfSs7MpNotAssocWithPlaceNotify

Recovery:

1. Set the MD-IWF admin state to Disabled on the SS7-MP Server.
2. If the Server is not associated with an AppWorks place, add the Server to an appropriate AppWorks Place. Then set the MD-IWF admin state to Enabled on the SS7-MP Server.

3. Contact *My Oracle Support (MOS)* for further assistance.

33065 - MD-IWF Resource Exhaustion

Event Group: MIWF

Description: MD-IWF Application is unable to process a message due to resource exhaustion.

Severity: Info

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfResourceExhaustionNotify

Recovery:

1. Check to see if any of the following resource utilization alarms are present on the SS7-MP. If so, follow the steps specified for the given alarm.

   - *33053 - MD-IWF DiamTrans Task Queue Utilization*
   - *33054 - MD-IWF MapTrans Task Queue Utilization*
   - *33055 - MD-IWF DAMPInterface Task Queue Utilization*
   - *33058 - MD-IWF DiamToMap PTR Utilization*
   - *33059 - MD-IWF MapToDiam PTR Utilization*
   - *22202 - PDU Buffer Pool Utilization*

2. Contact *My Oracle Support (MOS)* for assistance if needed.

33066 - MD-IWF orphan Diameter Answer message received

Event Group: MIWF

Description: MD-IWF Application received a Diameter Answer message for which no Pending Transaction record exists.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfOrphanDiamAnswerNotify

Recovery:

1. When MD-IWF sends a Diameter Request message to a DA-MP, it allocates a PTR and starts a timer (value is user configurable). The pending transaction is abandoned if a Diameter Answer response is not received within the user-configurable time limit. If this event is occurring frequently, the timer may be set too low. The Diameter Response Timeout value can be viewed via the **Main Menu** > **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options** NO GUI Screen.

2. Contact *My Oracle Support (MOS)* for assistance if needed.

33067 - MD-IWF orphan MAP Response message received

Event Group: MIWF

Description: MD-IWF Application received a MAP response message for which no Pending Transaction record exists.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfOrphanMapResponseNotify

Recovery:

1. If this event is occurring frequently, the configurable MAP Response timer may be set too low. The MAP Response Timeout value can be viewed via the NO GUI **Main Menu** > **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.

2. Contact *My Oracle Support (MOS)* for assistance if needed.

33068 - MD-IWF MAP Response timeout

Event Group: MIWF

Description: MD-IWF Application sent a MAP request message to the SS7 network, but timed out waiting for the MAP response.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfMapResponseTimeoutNotify

Recovery:

1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. It is possible that the MAP Response Timeout value is set too low.

2. The configured MAP Response Timeout value can be viewed via **Main Menu** > **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.

3. Contact *My Oracle Support (MOS)* for assistance if needed.

33069 - MD-IWF Diameter Answer timeout

Event Group: MIWF

Description: MD-IWF Application sent a Diameter Request message to the DA-MP, but timed out waiting for the Diameter Answer.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamAnswerTimeoutNotify

Recovery:

1. MAP-to-Diameter timeouts could be caused by delays in the Diameter network. It is possible that the Diameter Response Timeout value is set too low.
2. The configured Diameter Response Timeout value can be viewed via the NO GUI **Main Menu** > **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

33070 - MD-IWF Generated Diameter Answer error message due to Diameter Exception

Event Group: MIWF

Description: An error occurred while MD-IWF Application was processing a Diameter Request message, causing it generate a Diameter Answer error message.

Severity: Info

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfGeneratedDiamErrorAnswerNotify

Recovery:

Contact *My Oracle Support (MOS)* if assistance is needed.

33071 - MD-IWF Generated MAP Error Response due to MAP exception

Event Group: MIWF

Description: An error occurred while MD-IWF Application was processing a MAP request message, causing it generate a MAP response error message.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfGeneratedMapErrorResponseNotify

Recovery:

Contact *My Oracle Support (MOS)* if assistance is needed.

33072 - MD-IWF received TCAP Notice from SS7 network

Event Group: MIWF

Description: MD-IWF Application received a TCAP Notice from the SS7 network.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfTcapNoticeRecdNotify

Recovery:

A TC-Notice informs the TCAP Application that the network service provider is unable to provide the requested service.

33073 - MD-IWF admin state set to Enabled

Event Group: MIWF

Description: MD-IWF Application admin state was changed to Enabled on the SS7-MP

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfAdminStateEnabledNotify

Recovery:

No action required.

33074 - MD-IWF admin state set to Disabled

Event Group: MIWF

Description: MD-IWF Application admin state was changed to Disabled on the SS7-MP

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfAdminStateDisabledNotify

Recovery:

No action required.

33075 - MD-IWF received ComAgent error or DM-IWF NACK

Event Group: MIWF

Description: MD-IWF sent a Diameter Request message to DM-IWF that resulted in a ComAgent error / timeout or in a DM-IWF NACK.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfRcvdComAgtErrorOrDmiwfNckNotify

Recovery:

No action required.

33076 - MD-IWF received Diameter Anwer from unexpected DA-MP

Event Group: MIWF

Description: MD-IWF received Diameter Answer from unexpected DA-MP

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamAnsRcvdFrmUnexcpDaMpNotify

Recovery:

This error is not expected to occur. Contact *My Oracle Support (MOS)* for assistance if needed.

33077 - MD-IWF address translation failed

Event Group: MIWF

Description: MD-IWF was not able to perform address translation due to a lookup error in a configuration table, or else due to a missing or unexpected parameter / AVP

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfAddressTranslationFailedNotify

Recovery:

1. If address translation failed due to a lookup error in a configuration table, then analyze the configuration table to see if there is missing or incorrect data.
2. If address translation failed due to missing or unexpected MAP parameter or Diameter AVP value, then analyze the message to see if it is correct.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

33078 - MD-IWF received Diameter EIR message but Destination-Host AVP not present or not found in mapping table

Event Group: MIWF

Description: MD-IWF Application received a Diameter EIR message but the Destination-Host AVP was either 1)not present or 2)the Destination-Host AVP value was not present in table DiamIdentityGta.

Severity: Info

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamEirRecdDestHostNotPresentNotify

Recovery:

1. For case 1, investigate why the Destination-Host AVP was not present in the message. The DSR expects this AVP to be present.
2. For case 2, check to see if table DiamIdentityGta is configured correctly. It is possible the given Destination Host should be present in this table. This table is configured on the NO GUI via **Main Menu** > **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA**.
3. Contact *My Oracle Support (MOS)* for assistance if needed.

33079 - MD-IWF message translation failed

Event Group: MIWF

Description: MD-IWF attempt to perform message translation was unsuccessful.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfMessageTranslationFailedNotify

Recovery:

1. Based on the Translation Error Details, examine the message being translated and attempt to identify the reason for the failure
2. Contact *My Oracle Support (MOS)* for assistance if needed.

33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message

Event Group: MIWF

Description: EDL failure occurred while MD-IWF attempted to encode a Diameter message.

Severity: Info

Instance: mapiwf

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMdIwfDiamEirRecdDestHostNotPresentNotify

Recovery:

1. Examine the EDL error text in order to determine the reason for failure, If the encode failure is due to exceeding the maximum supported Diameter message size, and this event is being raised frequently, then it may be necessary to increase the engineering configurable parameter (DiameterMaxMessageSize in table MapIwfLongConfig) for maximum Diameter message size.

2. Contact *My Oracle Support (MOS)* for assistance if needed.

GLA (33100-33149)

This section provides information and recovery procedures for GLA alarms and events, ranging from 33100 to 33149, and lists the type of alarms and events that can occur on the system.

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

33100 - GLA Message Decoding Failure

Event Group: GLA

Description: Message received was rejected because of a decoding failure

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaMessageDecodingFailureNotify

Recovery:

1. While parsing the message, one of the following conditions occurred:

   - The message content was inconsistent with the "Message Length" in the message header.
   - The IMSI contained in the User-Name AVP was considered invalid due to length.

- The MSISDN contained in the MSISDN AVP was considered invalid due to length.

2. These protocol errors can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node. Collect a trace containing the GGR, and determine which node is causing the invalid data.

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

33101 - GLA Incorrect Application ID or Command Code

Event Group: GLA

Description: Message received was rejected because the Application ID was not GL (16777321) or the Command Code was not GGR (8388655).

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaIncorrectApplIdOrCmdCodeNotify

Recovery:

Examine the Application Routing Rules that direct traffic to GLA and verify that the Application ID is set to GL (16777321) and the Command Code is set to GGR (8388655) for all Application Routing Rules referring to GLA.

33102 - GLA Missing Subscriber ID

Event Group: GLA

Description: Message received was rejected because it did not contain and IMSI or an MSISDN in a Subscription-ID AVP

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaMissingSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.

2. If this condition is met, inspect each element between the GQC and GWS to determine if Subscriber information within the Request is being modified.

33103 - GLA Communication Agent Error

Event Group: GLA

Description: GLA was unable to communicate with the pSBR-Binding due to a communications error

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaComAgentErrorNotify

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. Examine the status of the Reporting Server's BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persist, contact *My Oracle Support (MOS)*.

33104 - GLA Duplicate Subscriber ID

Event Group: GLA

Description: Message received was rejected because it contained both a User-Name AVP and a MSISDN AVP

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaDuplicateSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.
2. Inspect each element between teh GQC and GQS to determine which node is inserting bot AVPs and correct that node so that only one AVP is included in the GGR.

33105 - Routing Attempt failed due to queue exhaustion

Event Group: GLA

Description: Message could not be routed because the internal "Answer Message Queue" to the DSR Relay Agent was full.

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaRoutingAttemptFailureDrlQueueExhNotify

Recovery:

1. This condition should not occur unless the DSR is experiencing severe congestion due to excessive traffic levels arriving on the DRL Answer Queue.
2. GL traffic should be diverted from the DA-MP to other DA-MPs in the DSR, or to another DSR.

33106 - GLA Communication Agent Timeout

Event Group: GLA

Description: GLA was unable to communicate with the pSBR-Binding and the query timed out.

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaComAgentTimeoutNotify

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. Examine the status of the Reporting Server's BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, contact *My Oracle Support (MOS)*.

33120 - Policy SBR Binding Sub-Resource Unavailable

Alarm Group: GLA

Description: GLA is unable to communicate with Policy SBR-Binding. One or more binding sub-resources are unavailable.

Severity:

- **Major:** When at least one server group that has a range of binding sub-resources is not available, but at least the minimum number of binding sub-resources is still available.
- **Critical:** When fewer than the minimum number of binding sub-resources are not available.

Instance: GLA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterGlaBindingSubresourceUnavailableNotify

Recovery

1. Monitor the Policy DRA Binding Resource on the GLA NO at **Main Menu** > **Configuration** > **Resource Domains**.
2. Determine if some of the pSBR-B MPs are unavailable or out-of-service. In this case, all DA-MPs and all pSBR-B MPs will also report ComAgent connection alarms.
3. Determine if there is a WAN outage. In this case, DA-MPs should also report ComAgent connection alarms to remote pSBR-Bs, and local pSBR-Bs should report ComAgent connection alarms to remote DA-MPs.
4. Determine if there is a network routing issue. In this case, one or a few DA-MPs may report a ComAgent connection against a limited number of pSBR-Bs.
5. If the problem persists, contact *My Oracle Support (MOS)* for assistance.

33121 - GLA pSBR-B Response Task Message Queue Utilization

Alarm Group: GLA

Description: GLA's pSBR-B Response Message Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxGlaResponseMsgQueue, GLA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterGlaRespTaskMessageQueueUtilizationNotify

Recovery

1. Determine if the GLA pSBR Response Task is mis-configured (Eg. Smaller response task queue size / fewer number of response task threads as compared to the request task threads).
2. Determine if the GLA pSBR Response Task has encountered a problem preventing it from processing messages from its Task Message Queue even if no additional congestion alarms are asserted.
3. If the problem persists, contact *My Oracle Support (MOS)* for additional assistance.

Chapter

5

Key Performance Indicators (KPIs)

Topics:

This section provides general information about KPIs, and lists the KPIs that can appear on the Status & Manage KPIs GUI page.

General KPIs information

This section provides general information about KPIs, the Status and Manage KPI page, and how to view KPIs.

KPIs overview

Key Performance Indicators (KPIs) allow the user to monitor system performance data, including CPU, memory, swap space, and uptime per server. This performance data is collected from all servers within the defined topology.

The KPI display function resides on all OAM servers. Servers that provide a GUI connection rely on KPI information merged to that server. The Network OAMP servers maintain status information for all servers in the topology. System OAM servers have reliable information only for servers within the same network element.

The Status and Manage KPIs page displays performance data for the entire system. KPI data for the entire system is updated every 60 seconds. If data is not currently being collected for a particular server, the KPI for that server will be shown as Unk for "Unknown".

KPIs

The **Status & Manage > KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server.

KPIs server elements

This table describes KPIs that appear regardless of server role.

Table 17: KPIs Server Elements

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

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

Viewing KPIs

Use this procedure to view KPI data.

1. Select **Status & Manage > KPIs**.

   The **Status & Manage KPIs** page appears with the **Server** tab displayed. For details about the KPIs displayed on this page, see the application documentation.

2. Click to select an application tab to see KPI data relevant to the application.

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

KPIs data export elements

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

Table 18: Schedule KPI Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-).

Element	Description	Data Input Notes
		Description must begin with an alphanumeric character.
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting KPIs

You can schedule periodic exports of security log data from the **KPIs** page. KPI data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **KPIs** page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transfered to an alternate location using the Export Server feature. For more information about using **Export Server**, see *Data Export*.

Use this procedure to schedule a data export task.

1. Select **Status & Manage > KPIs**.

   The **KPIs** page appears.

2. If necessary, specify filter criteria and click **Go**.
   The KPIs are displayed according to the specified criteria.

3. Click **Export**.
   The **Schedule KPI Data Export** page appears.

4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *KPIs data export elements* .

5. Select the **Export Frequency**.

6. If you selected Hourly, specify the **Minutes.**

7. Select the **Time of Day**.

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

8. Select the **Day of Week**.

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

9. Click **OK** or **Apply** to initiate the KPI export task.

From the **Status & Manage > Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see *Displaying the file list*.

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

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

Computer Aided Policy Making (CAPM) KPIs

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

Table 19: CAPM KPIs

Variable	Description
Processing time [ms]	Average processing time of Rule Template on a per Rule Template basis.
Active Templates	Number of Rule Templates that are in Active state.
Test Templates	Number of Rule Templates that are in Test state.
Development Templates	Number of Rule Templates that are in Development state.

Charging Proxy Application (CPA) KPIs

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

Table 20: Charging Proxy Application (CPA) KPIs

Variable	Description
CPA Answer Message Rate	Track the average number of Answer messages processed per second by the CPA application.
CPA Ingress Message Rate	Track the average number of Diameter messages received per second by the CPA application.
CPA Request Message Rate	Track the average number of Request messages processed per second by the CPA application.

Variable	Description
cSBR Query Error Rate	Track the average number of errors received per second by the CPA application when attempting to query (read, create, update, delete) SBR.
cSBR Query Rate	Track the average number of SBR Queries sent per second by the CPA application.

Communication Agent (ComAgent) KPIs

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

Table 21: Communication Agent KPIs

Variable	Description
User Data Ingress message rate	Average of User Data Ingress Message Rate (messages per second) utilization on a MP server. The Ingress Message Rate is the number of User Data StackEvents (messages) that ComAgent delivers to Application Layers Queue.

Diameter (DIAM) KPIs

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

Table 22: DIAM KPIs

Variable	Description
Ingress Trans Success Rate	Percentage of ingress peer-to-peer transactions successfully complete
MsgCopyTxQueueUtilization	Percentage of utilization of the Message Copy Tx Queue
Avg Rsp Time (ms)	Average time from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer
Routing Success Rate	Percentage of transactions successfully routed on first attempt

DM-IWF KPIs

The KPI values associated with DM-IWF are visible using **Main Menu** > **Status & Manage** > **KPIs**

Table 23: DM-IWF KPIs

Variable	Description
Ingress Msg Rate	Average number of MAP-Diameter Interworking messages processed per second on a DA-MP. This includes messages received from DRL and messages received from SS7-MPs.
Diameter-to-MAP Trans Msg Rate	Average number of Diameter-to-MAP transaction messages processed per second.
MAP-to-Diameter Trans Msg Rate	Average number of MAP-to-Diameter transaction messages processed per second.

GLA KPIs

The KPI values associated with GLA are visible using **Main Menu** > **Status & Manage** > **KPIs**

Variable	Description
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on an MP server for this DSR Application. The Ingress Message Rate is the number of ingress Diameter messages that are selected for processing by the ART and sent to the DSR Application for processing.
Success Message Rate	GLA Success Message Rate (messages per second) on an MP server. The Success Message Rate is the number of ingress Diameter messages that are processed by GLA and answered with a success (2xxx) result code).

IDIH KPIs

The KPI values associated with the IDIH will be visible via the GUI **Main Menu** > **Status & Manage** > **KPIs**

Variable	Description
DSR-DIH TTR Bandwidth (KB/sec)	Average bandwidth used by DSR in sending TTRs (including trace start and stop messages) to DIH in Kbytes per second

IP Front End (IPFE) KPIs

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

Table 24: IPFE KPIs

Variable	Description
CPU %	Total CPU used by the IPFE process
Memory Total	Absolute memory used by the IPFE process
Memory %	Percent memory used by the IPFE process
Mem. Heap	Total heap allocated by the IPFE process
IPFE Packets/Sec	The average number of packets per second the IPFE receives
IPFE MBytes/Sec	The average number of megabytes per second the IPFE receives

MD-IWF KPIs

The KPI values associated with MD-IWF are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Variable	Description
Ingress Message Rate	Average number of MAP-Diameter Interworking messages processed per second on a SS7-MP. Includes MAP msgs received from SS7 network, and Diameter msgs received from DA-MPs.
Diameter-to-MAP Ingress Msg Rate	Average number of MAP-Diameter Interworking messages processed per second that result from Diameter-originated transactions. Includes the initial Diameter Request msg and all resulting MAP msgs that are received.
MAP-to-Diameter Ingress Msg Rate	Average number of MAP-Diameter Interworking messages processed per second that result from MAP-originated transactions. Includes the initial

Variable	Description
	MAP Request msg and all resulting MAP and Diameter msgs that are received.
Diameter Ingress Message Rate	Average number of Diameter messages (both Requests and Answers) received per second from DA-MPs.
MAP Ingress Message Rate	Average number of MAP messages (both requests and responses) received per second from SS7 network.

Message Processor (MP) KPIs

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

Table 25: MP KPIs

Variable	Description
Avg Diameter Process CPU Util	Average percent Diameter Process CPU utilization (0-100%) on a MP server.
Avg IMR Offered	Average Ingress Offered message rate (messages per second) on a MP server . Offered message rate is number of ingress Diameter messages before any Ingress controls are applied.
Avg IMR Accepted	Average Ingress Accepted message rate (messages per second) on a MP server . Accepted message rate is number of routable messages accepted by MP after all Ingress controls are applied.
Avg Messsage Processing Load	Average message processing load (messages per second) on a MP server. The message processing load is the number of Diameter messages that are routed , including Reroutes and Msgcop.

Full Address Based Resolution (FABR) KPIs

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

Table 26: FABR KPIs

Variable	Description
Ingress Message Rate	Ingress Message Rate (messages per second) utilization on a MP server for the FABR

Variable	Description
	Application. The Ingress Message Rate is the number of ingress Diameter messages that were successfully received by the FABR Application.
Resolved Message Rate	Resolved Message Rate (messages per second) utilization on a MP server. The Resolved Message Rate is the number of ingress Diameter messages that are successfully resolved to a Destination by the FABR application.
DP Response Time Average	Average DP response time is the average time (in milliseconds) it takes to receive a DP response after sending the corresponding DP query.

Policy and Charging Application (PCA) KPIs

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

Table 27: PCA KPIs

Variable	Description
PCA Ingress Message Rate	Number of Diameter messages including both requests and answers received by PCA from the Diameter Routing Layer per second.
P-DRA Ingress Message Rate	Number of Diameter messages including both requests and answers received by P-DRA from the Diameter Routing Layer per second.
OC-DRA Ingress Message Rate	Number of Diameter messages including both requests and answers received by OC-DRA from the Diameter Routing Layer per second.

Range Based Address Resolution (RBAR) KPIs

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

Table 28: RBAR KPIs

Variable	Description
Avg Resolved Message Rate	Average Resolved Message Rate (messages per second) utilization on a MP server. The Resolved Message Rate is the number of ingress Diameter messages that are successfully resolved to a

Variable	Description
	Destination by the Range Based Address Resolution application.
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on a MP server for this DSR Application. The Ingress Message Rate is the number of ingress Diameter messages that were successfully received by the DSR Application.

Session Binding Repository (SBR) KPIs

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

Note: SBR KPIs are only associated with the CPA function.

Table 29: SBR KPIs

Variable	Description
Current session bindings	Current number of session bindings
Mostly Stale session bindings	Number of session bindings found to be Mostly Stale during the previous audit
Session binding capacity	Number of session bindings as a percentage of the total capacity
Load Shed Rate	Rate (per second) at which queries (read, create, update, delete) are being shed due to congestion
Time to process query	Lifetime of a transaction in microseconds (time between query received and response sent)
Query rate	Number of queries (read, create, update, delete) processed per second

Subscriber Binding Repository (SBR) KPIs

The KPI values for SBR are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Table 30: SBR KPIs

Variable	Description
SBR Memory Utilization	SBR memory utilization (0-100%)
SBR Process CPU Utilization	SBR Process CPU Percent Utilization (0-100%)

Table 31: SBR-Binding KPIs

Variable	Description
SBR Policy Bindings	Number of Active SBR Policy Bindings
SBR Binding DB Read Rate	Number of SBR Binding DB reads per second
SBR Binding DB Write Rate	Number of SBR Binding DB writes per second

Table 32: SBR-Session KPIs

Variable	Description
SBR Policy Sessions	Number of Active SBR Policy Sessions
SBR Policy Session DB Read Rate	Number of SBR Policy Session DB reads per second
SBR Policy Session DB Write Rate	Number of SBR Policy Session DB writes per second
SBR Online Charging Sessions	Number of Active SBR Online Charging Sessions
SBR OC Session DB Read Rate	Number of SBR Online Charging Session DB reads per second
SBR OC Session DB Write Rate	Number of SBR Online Charging Session DB writes per second

SS7/Sigtran KPIs

Table 33: SS7/Sigtran KPIs

Variable	Description
SCCP Xmit Msgs/Sec	SCCP messages transmitted per second
SCCP Recv Msgs/Sec	SCCP messages received per second
SS7 Process CPU Utilization	The average percent of SS7 Process CPU utilization on an MP server.
Ingress Message Rate	The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue.
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent.
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received.

Glossary

B

BIOS

Basic Input-Output System

Firmware on the CPU blade that is executed prior to executing an OS.

C

CAPM

Computer-aided policy making

CCR-I

CCR Initial

Charging Proxy Application

A DSR Application that is responsible for sending and receiving Diameter accounting messages.

CMOS

Complementary Metal Oxide Semiconductor

CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.

ComAgent

Communication Agent

A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.

Communication Agent

See ComAgent.

C

CPA	Capability Point Code ANSI
	Charging Proxy Application - The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.
CPC	Capability Point Code
	A capability point code used by the SS7 protocol to identify a group of functionally related STPs in the signaling network.
CSV	Comma-separated values
	The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

DA-MP	Diameter Agent Message Processor
	A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.
DB	Database
	Daughter Board
	Documentation Bulletin
	Data bus

D

Diameter	Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. |
| DM-IWF | Diameter –MAP Interworking DSR Application, which translates Diameter messages into MAP messages |
| DNS | Domain Name Services

Domain Name System

A system for converting Internet host and domain names into IP addresses. |
| DP | Data Processor

The repository of subscriber data on the individual DSR node elements. The DP hosts the full address resolution database. |
| DRL | Diameter Routing Layer - The software layer of the stack that implements Diameter routing. |

D

DSR

Data Set Ready

Diameter Signaling Router

A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

Delete Subscriber Data Request

E

ETG

Egress Throttle Group (s)

F

FABR

Full Address Based Resolution

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

Full Address Based Resolution

See FABR.

G

GGR

Get-Gateway-Request A request for information for either an IMSI or an MSISDN. Only one subscriber (IMSI or MSISDN) is allowed to be queried per GGR. The GGR is generated by the GQC.

GLA

Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding

G

and session information is populated in the pSBR-B by the Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.

GQC	Gateway Query Client also known as Diameter Node
GUI	Graphical User Interface
	The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.
GWS	Gateway Screening
	Used at gateway STPs to limit access into the network to authorized users. A gateway STP performs inter-network routing and gateway screening functions. GWS controls access to nonhome SS7 networks. Only an MSU that matches predefined criteria in the EAGLE database is allowed to enter the EAGLE.

H

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

H

HP

Hewlett-Packard

I

IDIH

Integrated Diameter Intelligence Hub

IPFE

IP Front End

A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

K

KPI

Key Performance Indicator

L

LSP

Local Signaling Point

A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique primary/true point code within a particular SS7 Domain to an MP server.

M

M3RL

M3UA Routing Layer

A layer invented by Tekelec to enhance M3UA by adding a true routing layer.

MAP

Mated Application Part

Mobile Application Part

M

An application part in SS7
signaling for mobile
communications systems.

MD-IWF

MAP-Diameter Interworking SS7
Application, which translates MAP
messages into Diameter messages

MP

Message Processor - The role of the
Message Processor is to provide the
application messaging protocol
interfaces and processing.
However, these servers also have
OAM&P components. All Message
Processors replicate from their
Signaling OAM's database and
generate faults to a Fault
Management System.

N

NI

Network Indicator

NOAM

Network Operations,
Administration, and Maintenance

NTP

Network Time Protocol

NTP daemon

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

O

OAM

Operations, Administration, and
Maintenance

The application that operates the
Maintenance and Administration
Subsystem which controls the
operation of many products.

O

OID

Object Identifier

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

OOS

Out of Service

OPC

Originating Point Code

Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.

P

PCA

Point Code ANSI

PDU

Protocol Data Unit

PTR

Pending Transaction Record

R

Range Based Address Resolution

See RBAR.

RBAR

Range Based Address Resolution

A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, "Routing

R

Entity" Type, and Routing Entity address ranges.

Relay Agent

Diameter agent that forwards requests and responses to other Diameter nodes based on routing-related AVPs (such as Destination-Realm) and routing configuration. Because relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type.

REPL

Replication

RSP

Route Set Test - Prohibited message

Remote Signaling Point

Represents an SS7 network node (point code) that signaling must be sent to. An RSP has an SS7 domain (ANSI, ITUI, ITUN), a point code, and an optional Adjacent Server Group.

Remote Signaling Point

A logical element that represents a unique point code within a particular SS7 domain with which the SS7 application's Local Signaling Point interacts.

S

SBR

Subsystem Backup Routing

Session Binding Repository - A highly available, distributed

S

	database for storing Diameter session binding data
Session Binding Repository	See SBR.
SNMP	Simple Network Management Protocol.
	An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance
	Site Operations, Administration, and Maintenance
SOAP	Simple Object Access Protocol
STP	Signal Transfer Point
	The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.
	Spanning Tree Protocol
SW	Software
	Switch

T

T

TFA	TransFer Allowed (Msg)
TFC	Transfer Control
	TransFer Controlled (Msg)
	Transfer Congested
TFP	TransFer Prohibited (Msg)
	A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.
TFR	Transfer Restricted
TPC	True Point Code
TSA	Target Set Address
	An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.