# Table of Contents

## Chapter 1: Introduction

- Overview .................................................................................................................. 10
- Scope and Audience .................................................................................................. 10
- Manual Organization .................................................................................................. 10
- Documentation Admonishments .................................................................................. 11
- Related Publications .................................................................................................. 11
- Locate Product Documentation on the Oracle Technology Network Site .................. 11
- Customer Training ..................................................................................................... 12
- My Oracle Support (MOS) ......................................................................................... 12
- Emergency Response ................................................................................................ 13

## Chapter 2: User Interface Introduction

- User interface organization ....................................................................................... 15
  - User Interface Elements ......................................................................................... 15
  - Main menu options ................................................................................................. 16
- Common Graphical User Interface Widgets ............................................................... 17
  - System Login Page ................................................................................................. 17
  - Main Menu Icons ................................................................................................... 19
  - Work Area Displays ............................................................................................... 20
  - Customizing the Splash Page Welcome Message .................................................. 22
  - Column headers (sorting) ..................................................................................... 23
  - Page Controls ........................................................................................................ 23
  - Optional Layout Element Toolbar ......................................................................... 24
  - Filters .................................................................................................................... 25
  - Auto refresh controls ............................................................................................ 27
  - Pause Updates ....................................................................................................... 27
  - Max Records Per Page Controls ........................................................................... 28
  - Message display .................................................................................................... 28

## Chapter 3: Alarms and Events

- General alarms and events information .................................................................... 30
  - Alarms and events overview .................................................................................. 30
  - Alarms formatting information .............................................................................. 31
Chapter 4: Key Performance Indicators (KPIs) ................................. 260
  General KPIs information ................................................................. 261
  KPIs overview .................................................................................. 261
  KPIs .................................................................................................. 261
  Viewing KPIs ................................................................................... 261
  KPIs data export elements ............................................................... 261
  Exporting KPIs ................................................................................ 262
List of KPIs .......................................................................................... 263
  KPIs server elements ......................................................................... 263
  Process-based KPIs .......................................................................... 264
  UDRBE KPIs ...................................................................................... 265
  UDRFE KPIs ...................................................................................... 267
  UDR RAS and XSAS Provisioning Related KPIs............................... 267

Chapter 5: Measurements .................................................................... 270
  General measurements information .................................................. 271
  Measurements .................................................................................. 271
  Measurement elements ..................................................................... 272
# List of Figures

- **Figure 1**: Oracle System Login ................................................................. 18
- **Figure 2**: Paginated table ........................................................................... 20
- **Figure 3**: Scrollable table ........................................................................... 20
- **Figure 4**: Form page ................................................................................... 21
- **Figure 5**: Tabbed pages ............................................................................... 21
- **Figure 6**: Tabbed pages ............................................................................... 22
- **Figure 7**: Report output .............................................................................. 22
- **Figure 8**: Sortable and Non-sortable Column Headers ............................... 23
- **Figure 9**: Optional Layout Element Toolbar ........................................... 24
- **Figure 10**: Automatic Error Notification ............................................... 24
- **Figure 11**: Examples of Filter Styles ......................................................... 25
- **Figure 12**: Flow of Alarms ......................................................................... 30
- **Figure 13**: Alarm Indicators Legend ......................................................... 31
- **Figure 14**: Trap Count Indicator Legend ................................................... 31
- **Figure 15**: Breaker Panel LEDs ................................................................. 235
- **Figure 16**: Breaker Panel Setting ............................................................... 236
# List of Tables

Table 1: Admonishments .................................................................................................................................11

Table 2: User Interface elements ..........................................................................................................................15

Table 3: Main Menu Options ..............................................................................................................................16

Table 4: Main Menu icons ................................................................................................................................19

Table 5: Example Action buttons .........................................................................................................................23

Table 6: Submit buttons .......................................................................................................................................24

Table 7: Filter Control elements ..........................................................................................................................26

Table 8: Alarm/Event ID Ranges ..........................................................................................................................32

Table 9: Alarm and Event Types ........................................................................................................................32

Table 10: Schedule Active Alarm Data Export Elements ......................................................................................34

Table 11: Data Export Elements ........................................................................................................................36

Table 12: Schedule Security Log Data Export Elements .....................................................................................40

Table 13: Active Tasks Elements ........................................................................................................................41

Table 14: Active Tasks Report Elements .............................................................................................................44

Table 15: Scheduled Tasks Elements ..................................................................................................................45

Table 16: Schedule Event Data Export Elements ................................................................................................47

Table 17: Schedule KPI Data Export Elements ....................................................................................................262

Table 18: KPIs Server Elements ........................................................................................................................264

Table 19: Process-based KPIs ..............................................................................................................................264

Table 20: UDRBE KPIs .......................................................................................................................................265

Table 21: UDRFE KPIs .......................................................................................................................................267

Table 22: Provisioning KPIs .................................................................................................................................267
Table 23: Measurements Elements...............................................................................................................272
Table 24: Schedule Measurement Data Export Elements..................................................................................273
Table 25: OAM Alarm measurements.............................................................................................................276
Table 26: OAM System measurements.............................................................................................................276
Table 27: ESPR Measurements......................................................................................................................278
Table 28: UDRFE Measurements....................................................................................................................299
Table 29: UDR RAS and XSAS Provisioning Related Measurements..............................................................319
Introduction

The Introduction section explains the purpose and organization of the documentation, defines the document's audience and admonishments, and provides information about technical support, training, and how to locate related publications.

Topics:

- Overview.....10
- Scope and Audience.....10
- Manual Organization.....10
- Documentation Admonishments.....11
- Related Publications.....11
- Locate Product Documentation on the Oracle Technology Network Site.....11
- Customer Training.....12
- My Oracle Support (MOS).....12
- Emergency Response.....13
Overview

This documentation provides information about the Oracle Communications User Data Repository (UDR) alarms and events, corrective maintenance procedures, and other information used in maintaining the system, including:

- 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 events history
- List of alarms
- Information relevant to understanding Key Performance Indicators (KPIs) in the application
- The procedure for viewing KPIs
- List of KPIs
- Information relevant to understanding measurements in the application
- Measurement report elements, and the procedures for printing and exporting measurements
- List of measurements by function

Scope and Audience

This reference guide provides preventive and corrective procedures that aid personnel in maintaining the UDR platform. These procedures are used in response to a system alarm or output message, and are used to aid in the detection, isolation, and repair of faults.

Note: Some of the UDR components are shared by other applications in the product line. For this reason, the documentation for the shared components may include references to these other applications, and/or describe GUI options not visible or applicable to UDR. For example, DSR applications (such as RBAR, FABR, CPA, and Policy DRA) and IPFE are currently not used by UDR, so you may ignore references to these applications.

Manual Organization

Information in this document is organized into the following sections:

- *Introduction* contains general information about this documentation, including how to contact My Oracle Support (MOS), and how to Locate Product Documentation on the Oracle Technology Network Site.
- *User Interface Introduction* describes the organization and usage of the application’s user interface.
- *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 by KPI type, then alphabetically by KPI name.
- *Measurements* provides detailed measurement information, organized alphabetically by measurement category.
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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![DANGER]</td>
<td>Danger: (This icon and text indicate the possibility of personal injury.)</td>
</tr>
<tr>
<td>![WARNING]</td>
<td>Warning: (This icon and text indicate the possibility of equipment damage.)</td>
</tr>
<tr>
<td>![CAUTION]</td>
<td>Caution: (This icon and text indicate the possibility of service interruption.)</td>
</tr>
<tr>
<td>![TOPPLE]</td>
<td>Topple: (This icon and text indicate the possibility of personal injury and equipment damage.)</td>
</tr>
</tbody>
</table>

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 http://www.adobe.com.

2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link.
   The Oracle Communications Documentation page appears with Tekelec shown near the top.
4. Click the Oracle Communications Documentation for Tekelec Products link.
5. Navigate to your Product and then the Release Number, and click the View link (the Download link will retrieve the entire documentation set).
   A list of the entire documentation set for the selected product and release appears.
6. To download a file to your location, right-click the PDF link, select Save target as, and save to a local folder.

Customer Training

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

http://education.oracle.com/communications

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](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:

- User interface organization.....15
- Common Graphical User Interface Widgets.....17

This section describes the organization and usage of the application's 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 the application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to the application and its functions.

User Interface Elements

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

<table>
<thead>
<tr>
<th>Element</th>
<th>Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>Top bar across the web page</td>
<td>Displays the company name, product name and version, and the alarm panel.</td>
</tr>
<tr>
<td>Banner</td>
<td></td>
<td>The left side of the banner just above the Main Menu provides the following session information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The HA state of the machine to which the user is connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The role of the machine to which the user is connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The right side of the banner:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Shows the user name of the currently logged-in user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provides a link to log out of the GUI.</td>
</tr>
<tr>
<td>Session Banner</td>
<td>Next bar across the top of the web page</td>
<td></td>
</tr>
<tr>
<td>Main Menu</td>
<td>Left side of screen, under banners</td>
<td>A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To display submenu items, click the plus character, the folder, or anywhere on the same line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.</td>
</tr>
<tr>
<td>Work Area</td>
<td>Right side of panel under status</td>
<td>Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls</td>
</tr>
</tbody>
</table>
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 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

This table describes all main menu user interface options. Note that user documentation for the Administration, Configuration, Alarms & Events, Security Log, Status & Manage, and Measurements menu options is available in the Operations, Administration, and Maintenance (OAM) section of the documentation.

**Note:** The menu options that appear can differ according to the permissions assigned to a user's log-in account, as well as to the type of server the user is logged into. For example, the Administration menu options would not appear on the screen of a user who does not have administrative privileges. Similarly, when the user is accessing the GUI from a Network Operations, Administration, and Provisioning (NOAMP) server, the Diameter menu option does not appear.

### Table 3: Main Menu Options

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>The Administration menu allows you to:</td>
</tr>
<tr>
<td></td>
<td>• Set up and manage user accounts</td>
</tr>
<tr>
<td></td>
<td>• Prepare, initiate, monitor, and complete upgrades</td>
</tr>
<tr>
<td></td>
<td>• View the software versions report</td>
</tr>
<tr>
<td></td>
<td>• Configure group permissions</td>
</tr>
<tr>
<td></td>
<td>• View session information</td>
</tr>
<tr>
<td></td>
<td>• Authorize IP addresses to access the user interface</td>
</tr>
<tr>
<td></td>
<td>• Configure options including, but not limited to,</td>
</tr>
<tr>
<td></td>
<td>password history and expiration, login message, welcome message, and</td>
</tr>
<tr>
<td></td>
<td>the number of failed login attempts before an account is disabled</td>
</tr>
</tbody>
</table>
User Interface Introduction

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Function</th>
</tr>
</thead>
</table>
|                | • Configure SNMP services  
|                | • Configure Export Servers  
|                | • Configure Domain Name Services  
| Configuration  | Provides access to configuring network elements, servers, server groups, and systems.                                                  |
| Alarms & Events| Lists active alarms and alarm history.                                                                                                |
| Security Log   | Allows you to view and export security log data.                                                                                      |
| Status & Manage| Allows you to monitor the statuses of server processes, both collectively and individually, as well as perform actions required for server maintenance. Also allows you to view the status of file management systems, and to manage data files on servers throughout the system. |
| Measurements   | Allows you to view, modify, import, and export measurement data.                                                                          |
| Communication Agent | Provides infrastructure features and services for enabling inter-server communication.                                               |
| Diameter Common| Allows you to configure network identifiers and MP profiles, and export and import configuration data.                                  |
| Diameter       | Allows you to configure topology hiding and import and export diameter interface settings.                                               |
| UDR            | Allows you to configure options for the UDR, URDBE, and subscriber entities. Allows you to perform maintenance on subscriber queries, connections, the command log and to view the import, export, and subscribing client status. |

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.

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

Before logging in, the System Login page appears. You can create a login message that appears just below the Log In button on the System Login page.

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.

**Supported Browsers**

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

**Main Menu Icons**

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

**Table 4: Main Menu icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Folder" /></td>
<td>Folder</td>
<td>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 (-) collapses the folder.</td>
</tr>
<tr>
<td><img src="image" alt="Config File" /></td>
<td>Config File</td>
<td>Contains operations in an Options page.</td>
</tr>
<tr>
<td><img src="image" alt="File with Magnifying Glass" /></td>
<td>File with Magnifying Glass</td>
<td>Contains operations in a Status View page.</td>
</tr>
<tr>
<td><img src="image" alt="File" /></td>
<td>File</td>
<td>Contains operations in a Data View page.</td>
</tr>
<tr>
<td><img src="image" alt="Multiple Files" /></td>
<td>Multiple Files</td>
<td>Contains operations in a File View page.</td>
</tr>
<tr>
<td><img src="image" alt="File with Question Mark" /></td>
<td>File with Question Mark</td>
<td>Contains operations in a Query page.</td>
</tr>
<tr>
<td><img src="image" alt="User" /></td>
<td>User</td>
<td>Contains operations related to users.</td>
</tr>
<tr>
<td><img src="image" alt="Group" /></td>
<td>Group</td>
<td>Contains operations related to groups.</td>
</tr>
<tr>
<td><img src="image" alt="Help" /></td>
<td>Help</td>
<td>Launches the Online Help.</td>
</tr>
<tr>
<td><img src="image" alt="Logout" /></td>
<td>Logout</td>
<td>Logs the user out of the user interface.</td>
</tr>
</tbody>
</table>
Work Area Displays

In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

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.

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.

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.
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 populate on the page. Retrieve is always the default for tabbed pages.

<table>
<thead>
<tr>
<th>Entire Network</th>
<th>System.CPU_CoreUtilPct_Average</th>
<th>System.CPU_CoreUtilPct_Peak</th>
<th>System.CPU_DiskUtilPct_Average</th>
<th>System.CPU_DiskUtilPct_Peak</th>
<th>System.RAM_UtilPct_Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOAMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Timestamp** | **System CPU UtilPct Average** | **System CPU UtilPct Peak** | **System Disk UtilPct Average** | **System Disk UtilPct Peak** | **System RAM UtilPct Average**

- **10/22/2009 19:45**: 6.764068 44 0.520000 1 7.993907
- **10/22/2009 20:00**: 7.143644 25 0.520000 1 8.523622
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 19:00:55 2009 UTC
User: guadmin

<table>
<thead>
<tr>
<th>Username</th>
<th>Date of Last Login</th>
<th>Days Since Last Login</th>
<th>Account Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>guadmin</td>
<td>2009-06-19 19:00:17</td>
<td>0</td>
<td>enabled</td>
</tr>
</tbody>
</table>

End of User Account Usage Report

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 using this procedure.

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)**

Some column headers are links that, when clicked, sort the table by that column. Sorting does not affect filtering. Column headers that are black and group column headers are not sortable.

<table>
<thead>
<tr>
<th>Sortable column</th>
<th>Non-sortable column (group header)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status about ServerID</td>
<td>Replication Channel Status</td>
</tr>
</tbody>
</table>

*Figure 8: Sortable and Non-sortable Column Headers*

**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**

<table>
<thead>
<tr>
<th>Action button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert</td>
<td>Inserts data into a table.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits data within a table.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes data from table.</td>
</tr>
<tr>
<td>Change</td>
<td>Changes the status of a managed object.</td>
</tr>
</tbody>
</table>

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

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

Optional Layout Element Toolbar

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

![Optional Layout Element Toolbar](image)

Figure 9: 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.

![Automatic Error Notification](image)

Figure 10: 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.

![Filter Styles Example](image)

**Figure 11: Examples of Filter Styles**
Filter Control Elements
This table describes filter control elements of the user interface.

Table 7: Filter Control elements

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Displays an exact match.</td>
</tr>
<tr>
<td>!=</td>
<td>Displays all records that do not match the specified filter parameter value.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Displays all records with a parameter value that is greater than the specified value.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Displays all records with a parameter value that is greater than or equal to the specified value.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Displays all records with a parameter value that is less than the specified value.</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Displays all records with a parameter value that is less than or equal to the specified value.</td>
</tr>
<tr>
<td>Like</td>
<td>Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.</td>
</tr>
<tr>
<td>Is Null</td>
<td>Displays all records that have a value of Is Null in the specified field.</td>
</tr>
</tbody>
</table>

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 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. Click **Go** to filter on the selection, or click **Reset** to clear the selection.
   Records are displayed according to the specified criteria.

**Auto refresh controls**

Auto refresh controls are widgets that control the rate at which the Page Area refreshes on some pages. They are located in the Page Control Area on the right side. Auto refresh can be set to 15 seconds or 30 seconds, and it can be turned off. The changes take effect immediately.

Click one of the Auto Refresh options to set the auto refresh rate. Click the **Off** option to terminate automatic refreshing of the page.

**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.

Message display

A message appears at the top of the Work Area on a page when a process needs to communicate errors or information. When an event is in progress, a refresh link may be provided here so that you can refresh without having to use the browser's refresh function.

These are examples of some of the messages that can appear in a Work Area:

![Message Example 1](image1)

![Message Example 2](image2)

![Message Example 3](image3)
Chapter 3

Alarms and Events

Topics:
- General alarms and events information.....30
- List of alarms.....50

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 the following Operations, Administration, and Maintenance (OAM) and Platform Alarms sections are shared with other applications and may not appear in the UDR.
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 12: 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.

![Alarm Indicators Legend](image)

**Figure 13: Alarm Indicators Legend**

**Alarm formatting information**

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

The information provided about each alarm may include:

- **Alarm Type**: the type of alarm that has occurred. For a list of alarm types see *Table 9: Alarm and Event Types*.
- **Description**: describes the reason for the alarm
- **Severity**: the severity of the alarm
- **Instance**: where the alarm occurred, for example, GUI, <process name>, IP address, <server name>
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
- 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**

<table>
<thead>
<tr>
<th>Application/Process Name</th>
<th>Alarm ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM</td>
<td>10000-10999</td>
</tr>
<tr>
<td>IDIH</td>
<td>11500-11549</td>
</tr>
<tr>
<td>Provisioning (RAS, XSAS, and Prov-Misc)</td>
<td>13000-13100</td>
</tr>
<tr>
<td>UDR</td>
<td>13101-13500</td>
</tr>
<tr>
<td>ComAgent</td>
<td>19800-19899</td>
</tr>
<tr>
<td>EXG Stack</td>
<td>19900-19999</td>
</tr>
<tr>
<td>Diameter</td>
<td>22000-22999</td>
</tr>
<tr>
<td>CAPM</td>
<td>25000-25499</td>
</tr>
<tr>
<td>OAM Alarm Management</td>
<td>25500-25899</td>
</tr>
<tr>
<td>Platform</td>
<td>31000-32700</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Type Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUD</td>
<td>Audit</td>
</tr>
<tr>
<td>CAF</td>
<td>Communication Agent (ComAgent)</td>
</tr>
<tr>
<td>CAPM</td>
<td>Computer-Aided Policy Making (Diameter Mediation)</td>
</tr>
<tr>
<td>CFG</td>
<td>Configuration</td>
</tr>
<tr>
<td>COLL</td>
<td>Collection</td>
</tr>
</tbody>
</table>
### Type Name | Type
---|---
DB | Database
DIAM | Diameter
DISK | Disk
HA | High Availability
IF | Interface
IP | Internet Protocol
IPFE | IP Front End
LOG | Logging
MEAS | Measurements
MEM | Memory
OAM | Operations, Administration & Maintenance
PDRA | Policy DRA
PLAT | Platform
PROC | Process
PROV | Provisioning
NAT | Network Address Translation
RBAR | Range-Based Address Resolution
REPL | Replication
SCTP | Stream Control Transmission Protocol
SL | Selective Logging
SPR | Subscriber Profile Repository
STK | EXG Stack
SW | Software (generic event type)
UDR | User Data Request
UDRF | UDR Front End Application running on MP Server

### 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 NOAM or SOAM. Alarm collection is handled solely by NOAM 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

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
</table>
| 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. |
| 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 | Format: Scrolling list
Range: 0 to 59 |
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 transferred 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.
   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. For more information, see *Opening a file*.

---

**Data Export**

From the Data Export page you can set an export target to receive exported selected data. Several types of 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 security log files
- Exporting KPIs
- Exporting measurements reports

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 11: Data Export Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Name of export server.</td>
<td>Must be a valid hostname or a valid IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Data Input Notes</td>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None</td>
<td>Username</td>
<td>Username used to access the export server</td>
</tr>
<tr>
<td>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</td>
<td>Directory on Export Server</td>
<td>Directory path on the export server where the exported data files are to be transferred</td>
</tr>
<tr>
<td>Format: Textbox Range: Maximum length is 255 characters; valid value is any UNIX string. Default: None</td>
<td>Path to rsync on Export Server</td>
<td>Optional path to the rsync binary on the export server</td>
</tr>
<tr>
<td>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</td>
<td>Backup File Copy Enabled</td>
<td>Enables or disables the transfer of the backup files.</td>
</tr>
<tr>
<td>Format: Checkbox Default: Disabled (unchecked)</td>
<td>File Compression</td>
<td>Compression algorithm used when exported data files are initially created on the local host.</td>
</tr>
<tr>
<td>Format: Radio button Range: gzip, bzip2, or none Default: gzip</td>
<td>Upload Frequency</td>
<td>Frequency at which the export occurs</td>
</tr>
<tr>
<td>Format: Radio button Range: fifteen minutes, hourly, daily or weekly Default: weekly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
<td>Data Input Notes</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 |
| 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.

Exporting security log files

You can schedule periodic exports of security log data from the Security Log View History page. Security log 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 transferred to an alternate location using the Export Server feature. For more information about using Export Server, see Data Export.

Use this procedure to export security log files. Use this procedure to schedule a data export task.

   The View History page appears.
2. If necessary, specify filter criteria and click Go.
   The security log files are displayed according to the specified criteria.
3. Click Export.
   The Schedule Security Log Data Export page appears.
4. Enter the Task Name.
   For more information about Task Name, or any field on this page, see Security log data export elements.
5. Enter a Description for the export task.
6. Select the Export Frequency.
7. If you selected Hourly as the export frequency, select the Minute of each hour for the data export.
8. Select the Time of Day.
   Note: Time of Day is not an option if Export Frequency equals Once.
9. Select the Day of Week.
   Note: Day of Week is not an option if Export Frequency equals Once.
10. Click OK or Apply to initiate the security log 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
11. Click Export.
The file is exported.

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

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

If an export fails for any reason, an error message appears indicating this failure.

**Note:** Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export doesn’t start. You must wait until the other export is complete before you can begin your export.

**Security log data export elements**

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

**Table 12: Schedule Security Log Data Export Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
</table>
| 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.                      |                                                                                  |
| Export Frequency         | Frequency at which the export occurs                                        | Format: Radio button
|                          | Range: Fifteen Minutes, Once, Hourly, Weekly, or Daily
|                          | Default: Once                                                               |                                                                                  |
| Minute                   | If hourly or fifteen minutes is selected for Export Frequency, this is the minute of each hour when the data will be written to the export directory. | Format: Textbox or Scrolling List
|                          | Range: 0 to 59
|                          | Default: 0                                                                  |                                                                                  |
| Time of Day              | Time of day the export occurs                                               | Format: Scrolling List
|                          | Range: 15-minute increments
|                          | Default: 12:00 AM                                                            |                                                                                  |
| Day of Week              | Day of week on which the export occurs                                      | Format: Radio button                                                            |
Alarms and Events

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday</td>
<td></td>
<td>Default: Sunday</td>
</tr>
</tbody>
</table>

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 an **NE Name**.

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

4. Click **List Files**.
   The **Status & Manage Files** list page for the selected server displays all files stored in its file management storage area.
   All files stored on the selected server are displayed. The amount of available and used storage space appears at the bottom of the page.

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 Tasks** 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**

<table>
<thead>
<tr>
<th>Active Tasks Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Task ID</td>
</tr>
<tr>
<td>Name</td>
<td>Task name</td>
</tr>
</tbody>
</table>
### Active Tasks

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Current status of the task. Status values include: running, paused, completed, exception, and trapped.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time and date when the task was started</td>
</tr>
<tr>
<td>Update Time</td>
<td>Time and date the task's status was last updated</td>
</tr>
<tr>
<td>Result</td>
<td>Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.</td>
</tr>
<tr>
<td>Result Details</td>
<td>Details about the result of the task</td>
</tr>
<tr>
<td>Progress</td>
<td>Current progress of the task</td>
</tr>
</tbody>
</table>

#### 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:** 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**

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

**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 security log files
- Exporting KPIs
- Exporting measurements reports

Viewing scheduled tasks

Use this procedure to view the scheduled tasks.

1. Select Status & Manage > Tasks > Scheduled Tasks.
2. 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

<table>
<thead>
<tr>
<th>Scheduled Tasks Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>Name given at the time of task creation</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the task</td>
</tr>
<tr>
<td>Time of Day</td>
<td>The hour and minute the task is scheduled to run</td>
</tr>
<tr>
<td>Day-of-Week</td>
<td>Day of the week the task is scheduled to run</td>
</tr>
<tr>
<td>Network Elem</td>
<td>The Network Element associated with the task</td>
</tr>
</tbody>
</table>

Editing a scheduled task

Use this procedure to edit a scheduled task.

1. Select Status & Manage > Tasks > Scheduled Tasks.
2. The Scheduled Tasks page appears, and all scheduled tasks are displayed.
3. Select a task.
4. Click Edit.
5. The Data Export page for the selected task appears.
6. Edit the available fields as necessary.
7. See Scheduled Tasks elements for details about the fields that appear on this page.
8. 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.

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 NOAM or SOAM. Alarm collection is handled solely by NOAM 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 historical 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 16: Schedule Event Data Export Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
</table>
| 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. |
| Export Frequency  | Frequency at which the export occurs | Format: Radio button
|                   |                           | Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily
|                   |                           | Default: Once                                                                   |
### Data Input Notes

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minute</td>
<td>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.</td>
<td>Format: Scrolling list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 0 to 59</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Time of Day</td>
<td>Time of day the export occurs</td>
<td>Format: Time textbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 15-minute increments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 12:00 AM</td>
</tr>
<tr>
<td>Day of Week</td>
<td>Day of week on which the export occurs</td>
<td>Format: Radio button</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: Sunday, Monday, Tuesday,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wednesday, Thursday, Friday, or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saturday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Sunday</td>
</tr>
</tbody>
</table>

### 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 transferred 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.
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.

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 Opening a file.

Opening a file

Use this procedure to open a file stored in the file management storage area.

1. Select Status & Manage > Files.

The Status & Manage Files page appears.

2. Select an NE Name.

3. Click List Files.

The Status & Manage Files list page for the selected network element displays all files stored in its file management storage area.

4. Click the Filename of the file to be opened.

Your browser's File Download window appears.

5. Click Open to open the file.

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.

List of alarms

This section of the document provides a list of all alarms that can be raised by the system. They are in numeric order and are grouped by alarm type.

10000-10999 - Operations, Administration, and Maintenance

This section provides information and recovery procedures for Operations, Administration, and Maintenance (OAM) alarms, ranging from 10000-10999.

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.

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 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: awpss7OAGT CantMonitorTableNotify
Recovery:
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.
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.

10110 - Certificate About to Expire

**Alarm Group:** AUD

**Description:** The certificate expires within 30 days.

**Severity:** Minor
Instance: <CertificateName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: certificateAboutToExpire
Recovery:
   Contact My Oracle Support (MOS) for assistance.

10111 - Certificate Expired
Alarm Group: AUD
Description: The certificate is expired.
Severity: Major
Instance: <CertificateName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: certificateExpired
Recovery:
   Contact My Oracle Support (MOS) for assistance.

10112 - Certificate Cannot Be Used
Alarm Group: AUD
Description: The certificate cannot be used because the certificate is not available yet.
Severity: Major
Instance: <CertificateName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: certificateCannotBeUsed
Recovery:
   Contact My Oracle Support (MOS) for assistance.

10120 - Server Group Upgrade Started
Event Group: LOG
Description: The server group upgrade operation has started.
Severity: Info
Instance: <ServerGroupName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogSgUpgradeStart
Recovery:
   No action required.

10121 - Server Group Upgrade Cancelled - Validation Failed
Event Group: LOG
Description: The server group upgrade operation has been cancelled due to validation failure.
Severity: Info
Instance: <ServerGroupName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogSgUpgradeCancelled
Recovery:
   No action required.

10122 - Server Group Upgrade Successful
Event Group: LOG
Description: The server group upgrade operation completed successfully.
Severity: Info
Instance: <ServerGroupName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogSgUpgradeSuccess
Recovery:
   No action required.

10123 - Server Group Upgrade Failed
Event Group: LOG
Description: The server group upgrade operation failed.
Severity: Info
Instance: <ServerGroupName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogSgUpgradeFailed
Recovery:
   No action required.

**10124 - Server Group Upgrade Cancelled - User Request**

Event Group: LOG
Description: The user cancelled the server group upgrade operation.
Severity: Info
Instance: <ServerGroupName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogSgUpgradeCancelledUser
Recovery:
   No action required.

**10130 - Server Upgrade Started**

Event Group: LOG
Description: The server upgrade operation has started.
Severity: Info
Instance: <HostName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogServerUpgradeStart
Recovery:
   No action required.

**10131 - Server Upgrade Cancelled**

Event Group: LOG
Description: The server upgrade operation has been cancelled due to validation failure.
Severity: Info
Instance: <HostName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogServerUpgradeCancelled
Recovery:
   No action required.

10132 - Server Upgrade Successful
Event Group: LOG
Description: The server upgrade operation completed successfully.
Severity: Info
Instance: <HostName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogServerUpgradeSuccess
Recovery:
   No action required.

10133 - Server Upgrade Failed
Event Group: LOG
Description: The server upgrade operation failed.
Severity: Info
Instance: <HostName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogServerUpgradeFailed
Recovery:
   No action required.

10134 - Server Upgrade Failed
Alarm Group: LOG
Description: The server upgrade operation failed.
Severity: Major
Instance: <HostName>
HA Score: Normal
Auto Clear Seconds: 0
OID: tekelecLogServerUpgradeFailAlm
Recovery:

1. If there are servers in the server group that have successfully upgraded, the user will need to individually restart the upgrade on that server. Navigate to the Upgrade page (Administration > Software Management > Upgrade).
2. Select the "Server Group" tab containing the server that raised the alarm.
3. Select the individual server(s) and then click the Server Upgrade button to start the upgrade on those servers.
   Note: Servers cannot be selected across tabs. If there are servers in multiple server groups, the user must restart the server upgrade for each additional "Server Group” tab.
4. If no servers in the group have been upgraded, the user can select the Auto Upgrade button to upgrade all servers in the server group. If a server upgrade has failed already, the alarm will be cleared when the server begins to upgrade.
   Note: The active server in the NO server group will never upgrade automatically.

10135 - Server Upgrade Canceled - User Request
Event Group: LOG
Description: The server upgrade was canceled by the user.
Severity: Info
Instance: <ServerGroupName>
HA Score: Normal
Throttle Seconds: 1
OID: tekelecLogServerUpgradeCancelledUser
Recovery: No action required.

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
Event Group: LOG
Description: SAML Login Successful
Severity: Info
Instance: N/A
HA Score: Normal
Throttle Seconds: 1
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
Event 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
Throttle Seconds: 1
OID: tekelecSamlLoginFailed
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 NOAM 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).

11500-11549 - IDIH

This section provides information and recovery procedures for Integrated Diameter Intelligence Hub (IDIH) alarms, which range from 11500 to 11549.

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.

**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. Tracing will resume once the danger of CPU congestion subsides.

**11501 - Trace Throttling Active**

**Alarm Group:** IDIH

**Description:** Troubleshooting trace has been throttled on some DA-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 HostName
Alarm Group: IDIH
Description: Unable to connect via ComAgent to remote DIH server with HostName
Severity: Minor
Instance: String of Configured DIH HostName
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterInvalidDihHostNameAlarmNotify
Recovery:  
   No action required
11506 - Invalid IDIH-Trace AVP

Alarm Group: IDIH

Description: An IDIH-Trace AVP has been received with an invalid format.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterInvalidIDIHTraceAvpNotify

Recovery:

1. If the message came from a peer that is not a DA-MP, verify that the peer is not modifying the AVP value (peers may retain the IDIH-Trace AVP unchanged, or remove it entirely, at their discretion).
2. If the message came from a peer that is a DA-MP, contact My Oracle Support (MOS).

11507 - Unable to run network trace at this site

Alarm Group: IDIH

Description: A network trace could not be run at this site because the connection or peer referenced by the trace scope value is not configured at this site. The trace will still run at sites that have this entity configured.

Severity: Info

Instance: <TraceName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterUnableToRunNetworkTraceAtThisSiteNotify

Recovery:

No action required; the trace will still run at all sites that have the indicated object configured at their site.

11508 - Network Trace Configuration Error

Alarm Group: IDIH

Description: An error occurred during configuration of the network trace. Please delete the trace definition.

Severity: Minor

Instance: <TraceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterNetworkTraceConfigurationErrorNotify
Recovery:
   Delete the network trace that raised the alarm.

11509 - Site Trace Configuration Error
Alarm Group: IDIH
Description: An error occurred during configuration of the site trace. Please delete the trace definition.
Severity: Minor
Instance: <TraceName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterSiteTraceConfigurationErrorNotify
Recovery:
   Delete the site trace that raised the alarm.

11510 - Network Trace Activation Error
Alarm Group: IDIH
Description: Network trace is not active on this site. A temporary error occurred during the activation of the network trace.
Severity: Minor
Instance: <TraceName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterNetworkTraceActivationErrorNotify
Recovery:
   No action required.

13000-13100 - PROV (UDR RAS, XSAS, and Prov-Misc)
This section provides information and recovery procedures for provisioning alarms (RAS, XSAS, and miscellaneous provisioning-related), ranging from 13000 - 13100. Alarms and events are recorded in a database log table.
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.

13000 - RAS Interface Disabled
Alarm Type: PROV
Description: Provisioning interface is manually disabled.
Severity: Critical
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: RasProvInterfaceDisabled
Recovery:
1. Manually enable the interface on the Provisioning Options page.
2. If the problem persists, contact *My Oracle Support (MOS)*.

13001 - No Remote RAS Client Connections
Alarm Type: PROV
Description: Provisioning interface is enabled and no remote provisioning clients are connected.
Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: RasProvNoRemoteConnections
Recovery:
1. Verify the provisioning interface is enabled and establish at least one remote RAS provisioning client connection.
2. If the problem persists, contact *My Oracle Support (MOS)*.

13002 - RAS Connection Failed
Alarm Type: PROV
Description: Provisioning client connection initialization failed due to an error. See the trace log for details (CID=<Connection ID>, IP=<IP Address>).
Severity: Major
Instance: Connection ID : IP Address
HA Score: Normal
Auto Clear Seconds: 300
OID: RasProvConnectionFailed
Recovery:
1. Wait 5 minutes for the alarm to automatically clear or establish a successful RAS connection.
2. If the problem persists, contact *My Oracle Support (MOS)*.
13003 - Invalid RAS Provisioning Configuration

Alarm Type: PROV
Description: Provisioning client connection initialization failed because the provisioning ports are the same.
Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: RasProvInvalidConfiguration
Recovery:
1. Change the ports to all be unique on the Provisioning Options page.
2. If the problem persists, contact My Oracle Support (MOS).

13010 - RAS Connection Established

Alarm Type: PROV
Description: This event is generated each time a remote provisioning client successfully establishes a REST connection. (Remote client connection established -- CID Connection ID, IP IP Address)
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: RasProvConnectionEstablished
Recovery:
No action required.

13011 - RAS Connection Terminated

Alarm Type: PROV
Description: This event is generated each time a remote provisioning client connection terminates. (Remote client connection terminated -- CID Connection ID, IP IP Address)
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: RasProvConnectionTerminated
Recovery:
1. Attempt to re-establish the RAS connection.
2. If the problem persists, contact My Oracle Support (MOS).

**13012 - RAS Connection Denied**

**Alarm Type:** PROV  
**Description:** This event is generated each time a local or remote provisioning client initiated connection establishment is denied due to one of the following reasons:  
- Connection originating from an unauthorized IP address  
- Maximum number of allowed remote client connections have been reached  
**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** N/A  
**OID:** RasProvConnectionDenied  
**Recovery:**  
1. Determine the cause the issue using the following  
   - Is the IP address authorized?  
   - Has the maximum number of allowed remote client connections been reached?  
2. After resolving the underlying issue, attempt to reconnect the RAS connection.  
3. If the problem persists, contact My Oracle Support (MOS).

**13026 - XSAS Interface Disabled**

**Alarm Type:** PROV  
**Description:** Provisioning interface is manually disabled.  
**Severity:** Critical  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0  
**OID:** XsasProvInterfaceDisabled  
**Recovery:**  
1. Manually enable the interface if the Provisioning Interface was manually disabled.  
2. If the problem persists, contact My Oracle Support (MOS).

**13027 - No Remote XSAS Client Connections**

**Alarm Type:** PROV  
**Description:** No remote provisioning XSAS clients are connected.
Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: XsasProvNoRemote Connections
Recovery:
1. Verify the provisioning interface is enabled.
2. Establish at least one remote XSAS provisioning client connection.
3. If the problem persists, contact My Oracle Support (MOS).

13028 - XSAS Connection Failed
Alarm Type: PROV
Description: Provisioning client connection initialization failed due to an error. See the trace log for details. (CID=<Connection ID>, IP=<IP Address>).
Severity: Major
Instance: Connection ID : IP Address
HA Score: Normal
Auto Clear Seconds: 0
OID: XsasProvConnectionFailed
Recovery:
1. Wait 5 minutes for the alarm to automatically clear or establish a successful XSAS connection.
2. If the problem persists, contact My Oracle Support (MOS).

13029 - Invalid XSAS Provisioning Configuration
Alarm Type: PROV
Description: Provisioning client connection initialization failed because the provisioning ports are the same.
Severity: Major
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: XsasProvInvalidConfiguration
Recovery:
1. Change the ports to all be unique.
2. If the problem persists, contact My Oracle Support (MOS).
13035 - XSAS Connection Established

Alarm Type: PROV

Description: This event is generated each time a remote provisioning client successfully establishes a SOAP connection.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: XsasProvConnectionEstablished

Recovery:

No action required.

13036 - XSAS Connection Terminated

Alarm Type: PROV

Description: This event is generated each time a remote provisioning client connection terminates.

 Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: XsasProvConnectionTerminated

Recovery:

1. Attempt to re-establish the XSAS connection.
2. If the problem persists, contact My Oracle Support (MOS).

13037 - XSAS Connection Denied

Alarm Type: PROV

Description: This event is generated each time a local or remote provisioning client initiated connection establishment is denied due to one of the following reasons:

- Connection originating from an unauthorized IP address
- Maximum number of allowed remote client connections have been reached

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: XSASConnectionDenied
Recovery:
1. Determine the cause of the issue using the following:
   - Is the IP address authorized?
   - Has the maximum number of allowed remote client connections been reached?
2. After resolving the underlying issue, attempt to reconnect the XSAS connection.
3. If the problem persists, contact My Oracle Support (MOS).

13051 - Import Throttled
Alarm Type: PROV
Description: Provisioning import throttled to prevent overrunning database service processes.
Severity: Minor
Instance: provimport
HA Score: Normal
Auto Clear Seconds: 5
OID: ProvImportThrottled
Recovery:
1. Wait 5 seconds for throttling to subside.
2. If the problem persists, contact My Oracle Support (MOS).

13052 - Import Initialization Failed
Alarm Type: PROV
Description: Provisioning import failed due to initialization error. See the trace log for details.
Severity: Major
Instance: provimport
HA Score: Normal
Auto Clear Seconds: 43200
OID: ProvImport InitializationFailed
Recovery:
1. Correct the problem based on the error in the trace log.
2. Try the import again.
3. If the problem persists, contact My Oracle Support (MOS).

13053 - Import Generation Failed
Alarm Type: PROV
Description: Provisioning import failed due to failure to generate import log. See the trace log for error details.
Severity: Major
Instance: provimport
HA Score: Normal
Auto Clear Seconds: 43200
OID: ProvImport GenerationFailed
Recovery:
1. Correct the problem based on the error in the trace log.
2. Try the import again.
3. If the problem persists, contact My Oracle Support (MOS).

13054 - Import Transfer Failed
Alarm Type: PROV
Description: Provisioning import operation failed due to a file transfer error for the import log. Failed to transfer the file either to or from the remote host. See the trace log for details.
Severity: Major
Instance: provimport
HA Score: Normal
Auto Clear Seconds: 43200
OID: ProvImportTransferFailed
Recovery:
1. Correct the problem based on the error in the trace log.
2. Try the import again.
3. If the problem persists, contact My Oracle Support (MOS).

13055 - Import Successful
Alarm Type: PROV
Description: This event is generated each time an XML import is successful.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: ProvImportSuccessful
Recovery:
   No action required.
13056 - Export Initialization Failed

Alarm Type: PROV

Description: Provisioning export failed due to an initialization. See the trace log for details.

Severity: Major

Instance: provexport

HA Score: Normal

Auto Clear Seconds: 43200

OID: ProvExport InitializationFailed

Recovery:

1. Correct the problem based on the error in the trace log.
2. Try the export again.
3. If the problem persists, contact My Oracle Support (MOS).

13057 - Export Generation Failed

Alarm Type: PROV

Description: Provisioning export failed due to failure to generate export log. See the trace log for error details.

Severity: Major

Instance: provixport

HA Score: Normal

Auto Clear Seconds: 43200

OID: ProvExport GenerationFailed

Recovery:

1. Correct the problem based on the error in the trace log.
2. Try the export again.
3. If the problem persists, contact My Oracle Support (MOS).

13058 - Export TransferFailed

Alarm Type: PROV

Description: Provisioning export operation failed due to a file transfer error for the export log. The file failed to transfer either from or to the remote host. See the trace log for error details.

Severity: Major

Instance: provexport

HA Score: Normal

Auto Clear Seconds: 43200
**OID:** ProvExportTransferFailed

**Recovery:**
1. Correct the problem based on the error in the trace log.
2. Try the export again.
3. If the problem persists, contact *My Oracle Support (MOS).*

**13059 - Export Successful**

**Alarm Type:** PROV  
**Description:** This event is generated each time an XML export is successful.  
**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** N/A  
**OID:** ProvExportSuccessful  

**Recovery:**  
No action required.

**13061 - ERA ResponderFailed**

**Alarm Type:** PROV  
**Description:** Event responder failed (or event responder error cleared).  
**Severity:** Major  
**Instance:** era  
**HA Score:** Normal  
**Auto Clear Seconds:** 0  
**OID:** EraResponderFailed  

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

**13062 - RAS Process CPU Utilization Threshold Exceeded**

**Alarm Type:** PROV  
**Description:** The RAS Process CPU Utilization is approaching its maximum capacity. The alarm severity depends on the amount of CPU being used:

- Minor when utilization exceeds 60%
- Major when utilization exceeds 66%
- Critical when utilization exceeds 72%

**Severity:** Minor (Major, Critical)
13063 - RAS Process Memory Utilization Threshold Exceeded

Alarm Type: PROV

Description: The RAS Process Memory Utilization is approaching its maximum capacity. The alarm severity depends on the amount of memory being used:

- Minor when utilization exceeds 60%
- Major when utilization exceeds 66%
- Critical when utilization exceeds 72%

Severity: Minor (Major, Critical)

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: RasProcMemThresh

Recovery:

1. Reduce the REST interface provisioning rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)

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

13064 - XSAS Process CPU Utilization Threshold Exceeded

Alarm Type: PROV

Description: The XSAS Process CPU Utilization is approaching its maximum capacity. The alarm severity depends on the amount of CPU being used:

- Minor when utilization exceeds 60%

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: RasProcCpuThresh

Recovery:

1. Reduce the REST interface provisioning rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)

2. If the problem persists, contact My Oracle Support (MOS).
- Major when utilization exceeds 66%
- Critical when utilization exceeds 72%

**Severity:** Minor (Major, Critical)

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** XsasProcCpuThresh

**Recovery:**
1. Reduce the SOAP interface provisioning rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - \( \leq 57\% \) (clears Minor alarm)
   - \( \leq 63\% \) (clears Major alarm)
   - \( \leq 69\% \) (clears Critical alarm)

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

### 13065 - XSAS Process Memory Utilization Threshold Exceeded

**Alarm Type:** PROV

**Description:** The XSAS Process Memory Utilization is approaching its maximum capacity. The alarm severity depends on the amount of memory being used:

- Minor when utilization exceeds 60%
- Major when utilization exceeds 66%
- Critical when utilization exceeds 72%

**Severity:** Minor (Major, Critical)

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** XsasProcMemThresh

**Recovery:**
1. Reduce the SOAP interface provisioning rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - \( \leq 57\% \) (clears Minor alarm)
   - \( \leq 63\% \) (clears Major alarm)
   - \( \leq 69\% \) (clears Critical alarm)

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

### 13066 - UDRPROV Process CPU Utilization Threshold Exceeded

**Alarm Type:** PROV
**Description:** The UDRPROV Process CPU Utilization is approaching its maximum capacity. The alarm severity depends on the amount of CPU being used:

- Minor when utilization exceeds 60%
- Major when utilization exceeds 66%
- Critical when utilization exceeds 72%

**Severity:** Minor (Major, Critical)

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** udrProvProcCpuThresh

**Recovery:**

1. Reduce the UDRPROV interface provisioning rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)

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

**13067 - UDRPROV Process Memory Utilization Threshold Exceeded**

**Alarm Type:** PROV

**Description:** The UDRPROV Process Memory Utilization is approaching its maximum capacity. Alarms 13063 through 13066 may also appear at the same time to help identify which aspect of UDRPROV is having an issue. The alarm severity depends on the amount of memory being used:

- Minor when utilization exceeds 60%
- Major when utilization exceeds 66%
- Critical when utilization exceeds 72%

**Severity:** Minor (Major, Critical)

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** udrProvProcMemThresh

**Recovery:**

1. Reduce the UDRPROV interface provisioning rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)

2. If the problem persists, contact *My Oracle Support (MOS)*.
13101-13500 - User Data Repository

This section provides information and recovery procedures for UDR alarms and events, ranging from 13101-13500.

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.

13151 - AE Sh Create Failed

Alarm Type: UDR

Description: The creation of an auto-enrolled subscriber initiated by the reception of an Sh interface request failed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: xgSDMAeShCreateFailed

Recovery:

Contact My Oracle Support (MOS).

13152 - AE Sh Delete Failed

Alarm Type: UDR

Description: The deletion of an auto-enrolled subscriber initiated by the reception of an Sh interface request failed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: xgSDMAeShDeleteFailed

Recovery:

Contact My Oracle Support (MOS).

13153 - AE Prov Create Failed

Alarm Type: UDR

Description: The creation of an auto-enrolled subscriber initiated by the reception of a provisioning interface request failed.

Severity: Info
13154 - AE Convert Failed

Alarm Type: UDR

Description: The conversion of an auto-enrolled subscriber to a provisioned subscriber while provisioning failed.

Severity: Info

13155 - Scheduled Quota Reset Activity started

Alarm Type: UDR

Description: This event is generated each time the Quota Reset Scheduler starts running a new Quota Reset Task.

Severity: Info

13156 - Scheduled Quota Reset Activity completed

Alarm Type: UDR

Description: Scheduled Quota Reset scheduler completed executing a Quota Reset Task.

Severity: Info
13157 - Scheduled Quota Reset Activity aborted

Alarm Type: UDR
Description: This event is generated each time a user aborts a Quota Reset Task.
Severity: Info

13158 - Scheduled Quota Reset Activity paused

Alarm Type: UDR
Description: This event is generated each time the Quota Reset Scheduler pauses a task in RUNNING State due to UDRBE process congestion.
Severity: Info

13159 - Scheduled Quota Reset Activity resumed

Alarm Type: UDR
Description: This event is generated each time Quota Reset Scheduler resumes a task that was in PAUSED State due to UDRBE process congestion.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: QuotaResetActivityResumed
Recovery:
   No action required.

13251 - Subscription Record Full
Alarm Type: UDR
Description: The subscription record exceeded the maximum number of allowed notification subscriptions. When the maximum number of subscriptions is exceeded, the oldest subscription is purged to make room for the new subscription.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: xgSDMUdrSmSNOFull
Recovery:
1. Determine whether the cause of the event is one of the following:
   • Failures/restarts of an AS when a subscription was active (and thus an unsubscribe request was not sent)
   • Multiple subscribe requests from the same AS but with different user identities (IMSI, MSISDN, NAI etc.)
2. If these cases are valid, it may be possible to increase the maximum number of subscriptions allowed. Contact My Oracle Support (MOS).

13252 - Notification Late Response
Alarm Type: UDR
Description: A notification delivery response was received after timeout expired.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: xgSDMNotifLateResponse
Recovery:
   Contact My Oracle Support (MOS).
13253 - Notification No Valid Entity

Alarm Type: UDR

Description: The notification contains no valid entities. This event is most likely to occur if an entity is deleted from the Subscriber Entity Configuration, and a notification had been already written for the deleted entity.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: xgSDMNotifNoValidEntity

Recovery:

Contact *My Oracle Support (MOS)*.

13254 - AS Unavailable

Alarm Type: UDR

Description: The AS is unavailable. An AS becomes unavailable when a configurable number of attempts to deliver (different or the same) notifications to an AS fail, and the error indicates that the PNR did not reach the AS or could not be processed because the AS was too busy.

Severity: Major

Instance: AS address

HA Score: Normal

Auto Clear Seconds: 0

OID: xgSDMASUnavailable

Recovery:

1. Verify connectivity status between UDR and the AS, using the SO GUI.
2. Verify the connection states are as expected.
3. Check the event history logs for additional DIAM events or alarms from the MP server.
4. If the problem persists, contact *My Oracle Support (MOS)*.

13255 - Notification Table Full

Alarm Type: UDR

Description: The Notification table contains too many notifications that have not been delivered to ASs. This could be because:

- The rate at which notifications are being produced exceeds the rate at which they can be delivered.
- Notifications cannot be delivered to AS(s) because they are unavailable, and the notifications are being buffered for delivery at a later time.

The alarm severity depends upon the amount of the Notification Table being used:
• Minor when utilization exceeds 60%.
• Major when utilization exceeds 80%.
• Critical when utilization exceeds 95%.

Severity: Major (Minor, Critical)
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: xgSDMNotificationTableFull

Recovery:
1. Reduce the traffic rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   • <= 50% (clears Minor alarm)
   • <= 70% (clears Major alarm)
   • <= 90% (clears Critical alarm)

2. Verify that the application server(s) are available by checking the Main Menu > UDR > Maintenance > Subscribing Client Status page.

3. Depending on the reason that notifications cannot be delivered, it may be necessary to increase the number of notifications that can be stored by UDR. Contact My Oracle Support (MOS).

13351 - SNO Audit Complete
Alarm Type: UDR
Description: The SNO audit is complete.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: xgSDMAuditStatisticsReportSNO
Recovery:
   No action required.

13352 - SDO Audit Complete
Alarm Type: UDR
Description: The SDO audit is complete.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: xgSDMAuditStatisticsReportSDO
Recovery:  
No action required.

13354 - UDRBE Provisioning Task Message Queue Utilization

Alarm Type: UDR

Description: The UDRBE application’s provisioning task message queue is approaching its maximum capacity. This alarm should not occur when no other congestion alarms are asserted. The alarm severity depends upon the amount of the UDRBE provisioning task message queue being used:

- Minor when utilization exceeds 60%.
- Major when utilization exceeds 80%.
- Critical when utilization exceeds 95%.

Severity: Major (Minor, Critical)

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: UdrbeProvisioningTaskMessageQueueUtilization

Recovery:

1. Determine whether the traffic rate of the system is too high. If yes, reduce traffic rate to clear alarm. The alarm clears when utilization falls below these thresholds:
   - \( <= 50\% \) (clears Minor alarm)
   - \( <= 70\% \) (clears Major alarm)
   - \( <= 90\% \) (clears Critical alarm)

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

13355 - UDRBE Notification Task Event Queue Utilization

Alarm Type: UDR

Description: The UDRBE application’s notification task event queue is approaching its maximum capacity. This alarm should not occur when no other congestion alarms are asserted. The alarm severity depends upon the amount of the UDRBE notification task event queue being used:

- Minor when utilization exceeds 60%.
- Major when utilization exceeds 80%.
- Critical when utilization exceeds 95%.

Severity: Major (Minor, Critical)

Instance: N/A

HA Score: Normal
Auto Clear Seconds: 0
OID: UdrbeNotificationTaskEventQueueUtilization

Recovery:
1. Determine whether the traffic rate of the system is too high. If yes, reduce traffic rate to clear alarm. The alarm clears when utilization falls below these thresholds:
   • <= 50% (clears Minor alarm)
   • <= 70% (clears Major alarm)
   • <= 90% (clears Critical alarm)

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

13356 - UDRBE Udr Task Event Queue Utilization

Alarm Type: UDR

Description: The UDRBE application’s UDR task event queue is approaching its maximum capacity. This alarm should not occur when no other congestion alarms are asserted. The alarm severity depends upon the amount of the UDRBE UDR task event queue being used:
   • Minor when utilization exceeds 60%.
   • Major when utilization exceeds 80%.
   • Critical when utilization exceeds 95%.

Severity: Major (Minor, Critical)
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: UdrbeUdrTaskEventQueueUtilization

Recovery:
1. Determine whether the traffic rate of the system is too high. If yes, reduce traffic rate to clear alarm. The alarm clears when utilization falls below these thresholds:
   • <= 50% (clears Minor alarm)
   • <= 70% (clears Major alarm)
   • <= 90% (clears Critical alarm)

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

13357 - UDRBE Subscription Task Event Queue Utilization

Alarm Type: UDR

Description: The UDRBE application’s subscription task event queue is approaching its maximum capacity. This alarm should not occur when no other congestion alarms are asserted. The alarm severity depends upon the amount of the UDRBE subscription task event queue being used:
   • Minor when utilization exceeds 60%.
   • Major when utilization exceeds 80%.
• Critical when utilization exceeds 95%.

Severity: Major (Minor, Critical)
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: UdrbeSubscriptionTaskEventQueueUtilization

Recovery:
1. Determine whether the traffic rate of the system is too high. If yes, reduce traffic rate to clear alarm. The alarm clears when utilization falls below these thresholds:
   • <= 50% (clears Minor alarm)
   • <= 70% (clears Major alarm)
   • <= 90% (clears Critical alarm)
2. If the problem persists, contact My Oracle Support (MOS).

13358 - UDRBE Auto Enrollment Task Event Queue Utilization

Alarm Type: UDR

Description: The UDRBE application’s auto enrollment task event queue is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted. The alarm severity depends upon the amount of the UDRBE auto enrollment task event queue being used:
   • Minor when utilization exceeds 60%.
   • Major when utilization exceeds 80%.
   • Critical when utilization exceeds 95%.

Severity: Major (Minor, Critical)
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: UdrbeAutoEnrollmentTaskEventQueueUtilization

Recovery:
1. Determine whether the traffic rate of the system is too high. If yes, reduce traffic rate to clear alarm. The alarm clears when utilization falls below these thresholds:
   • <= 50% (clears Minor alarm)
   • <= 70% (clears Major alarm)
   • <= 90% (clears Critical alarm)
2. Examine the Alarm log to determine whether there are any problems preventing the UDRBE application task from processing messages from its auto enrollment task event queue.
3. If the problem persists, contact My Oracle Support (MOS).
13359 - Failed to register as a Routed Service user with ComAgent

Alarm Type: UDR

Description: The ComAgent Routed Service user registration failed. The UDRBE cannot use the ComAgent Routed Service for notification operations.

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: 0

OID: UdrbeComAgentRoutedServiceRegistrationFailure

Recovery:
1. Determine whether the configured ComAgent Routed Service name is correct.
2. Determine whether the ComAgent Routed Service is not configured in ComAgent.
3. If the problem persists, contact My Oracle Support (MOS).

13360 - The UDRBE Process CPU Utilization is approaching its maximum capacity

Alarm Type: UDR

Description: The UDRBE Process CPU Utilization is approaching its maximum capacity. The alarm severity depends on the amount of CPU being used:

- Minor when utilization exceeds 60%.
- Major when utilization exceeds 66%.
- Critical when utilization exceeds 72%.

Severity: Minor (Major, Critical)

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: UdrbeProcCpuThresh

Recovery:
1. Reduce the traffic rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)

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

13361 - UDRBE Process Memory Utilization Threshold Exceeded

Alarm Type: UDR
**Description:** The UDRBE Process Memory Utilization is approaching its maximum capacity. The alarm severity depends on the amount of memory being used:

- Minor when utilization exceeds 75%
- Major when utilization exceeds 80%
- Critical when utilization exceeds 85%

**Severity:** Minor (Major, Critical)

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** UdrbeProcMemThresh

**Recovery:**

1. Reduce the traffic rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   - <= 73% (clears Minor alarm)
   - <= 78% (clears Major alarm)
   - <= 83% (clears Critical alarm)

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

**13367 - UDRBE System Memory Utilization Threshold Exceeded**

**Alarm Type:** UDR

**Description:** System memory utilization threshold exceeded. Create and update provisioning, as well as auto-enrolled operations, are suspended when critical threshold is reached. Note that update requests for existing subscribers, triggered by a PUR message on the Sh interface, will continue to be processed, regardless of alarm status. The alarm severity depends on the amount of memory being used:

- Minor when system memory utilization exceeds 80%
- Major when system memory utilization exceeds 83%
- Critical when system memory utilization exceeds 85%

**Severity:** Minor (Major, Critical)

**Instance:** N/A

**HA Score:** Normal

**Auto Clear Seconds:** 0

**OID:** UdrbeSysMemThresh

**Recovery:**

1. The alarm clears when system memory utilization falls below these thresholds:
   - <= 79% (clears Minor alarm)
   - <= 82% (clears Major alarm)
   - <= 84% (clears Critical alarm)
2. Contact *My Oracle Support (MOS)*.

**13368 - Database Auditor: Audit/Clean Process Failed**

*Alarm Type:* UDR  
*Description:* Database Auditor's audit/clean process failed to complete the desired operation. Please refer to the result log for details.  
*Severity:* Major (Minor, Critical)  
*Instance:* N/A  
*HA Score:* Normal  
*Auto Clear Seconds:* 300  
*OID:* DbAuditorAuditFailed  
*Recovery:*  
   Manually start the audit/clean process from UDR > Maintenance > Database Auditor.

**13403 - Diameter Application ComAgent Event Queue Utilization**

*Alarm Type:* UDRF  
*Description:* Diameter Application's ComAgent Event Queue utilization is approaching its maximum capacity. This alarm appears when congestion occurs, and the severity of the alarm depends on how much queue capacity is being used:  
   - Minor when utilization >= 60%  
   - Major when utilization >= 80%  
   - Critical when utilization > 95%  
*Severity:* Minor (Major, Critical)  
*Instance:* N/A  
*HA Score:* Normal  
*Auto Clear Seconds:* 0  
*OID:* DiameterAppComAgentEventQueueUtilization  
*Recovery:*  
1. Reduce the traffic rate to clear the alarm after all pending stack events are processed by UDRBE. The alarm clears when the UDRFE application’s ComAgent Event Queue utilization falls below the maximum threshold:  
   - <= 50% (clears Minor alarm)  
   - <= 70% (clears Major alarm)  
   - <= 90% (clears Critical alarm)  
2. If the problem persists, contact *My Oracle Support (MOS).*
13404 - ComAgent Registration Failure

Alarm Type: UDRF

Description: COM Agent routing service registration or service notification registration failed. UDRFE cannot use the COM Agent service for database operations.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: SprfeComAgentRegistrationFailure

Recovery:

1. Restart the UDR process to clear the alarm:
   a) At the command line on the MP server, enter `pm.set off udr` (to stop process).
   b) At the command line on the MP server, enter `pm.set on udr` (to restart process).

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

13405 - Diameter Application Unavailable

Alarm Type: UDRF

Description: Diameter Application is unable to process any messages because it is Unavailable. A Diameter Application can become unavailable when:

- The Admin State is set to Disable with the forced shutdown option.
- The Admin State is set to Disable with the graceful shutdown option and the graceful shutdown timer expires.
- It reaches Congestion Level 3.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: DiameterApplicationUnavailable

Recovery:

1. Display and monitor the Diameter Application status by selecting Diameter > Maintenance > Applications in the SO GUI. Verify that the Admin State variable is set as expected.

2. A Diameter 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 Diameter Application can also become Unavailable when it reaches Congestion Level 3, if enabled. Note: This alarm will NOT be raised when the Diameter application is shutting down gracefully or application is in Disabled state. Only the Diameter 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)*.

**13406 - Diameter Application Degraded**

**Alarm Type:** UDRF  
**Description:** Unable to forward requests to the Diameter Application because it is Degraded. A Diameter Application becomes degraded when the Diameter Application becomes congested (if enabled).  
**Severity:** Major  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0  
**OID:** DiameterApplicationDegraded  
**Recovery:**  
1. Display and monitor the Diameter Application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify that the Admin State variable is set as expected.  
   A Diameter 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.  
   A Diameter Application can also become Unavailable when it reaches Congestion Level 3 (if enabled).  
   **Note:** This alarm will NOT be raised when the Diameter application is shutting down gracefully or application is in Disabled state. Only the Diameter Application operational status will be changed to Unavailable.

2. Check the Event History logs for additional DIAM events or alarms for this MP server.  
3. If the problem persists, contact *My Oracle Support (MOS)*.

**13407 - Diameter Application Request Task Queue Utilization**

**Alarm Type:** UDRF  
**Description:** The Diameter Application Request Task Queue Utilization is approaching its maximum capacity. The severity of the alarm depends on how much request queue capacity is being used:  
- Minor when utilization exceeds 60%  
- Major when utilization exceeds 80%  
- Critical when utilization exceeds 95%  
**Severity:** Minor (Major, Critical)  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0  
**OID:** DiameterAppRequestTaskQueueUtilization  
**Recovery:**
1. Display and monitor the Diameter Application status by selecting **Diameter > Maintenance > Applications** in the SO GUI. Verify that the Admin State variable is set as expected. The Diameter 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 misconfigured and is sending too much traffic to the Diameter Application. Verify the configuration by selecting **Diameter > Maintenance > Application Routing Rules**.

3. If no additional congestion alarms are asserted, the Diameter 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)**.

### 13408 - Diameter Application Answer Task Queue Utilization

**Alarm Type:** UDRF  
**Description:** The Diameter Application Answer Task Queue utilization is approaching its maximum capacity. The severity of the alarm depends on how much answer queue capacity is being used:

- Minor when utilization exceeds 60%
- Major when utilization exceeds 80%
- Critical when utilization exceeds 95%

**Severity:** Minor (Major, Critical)  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** 0  
**OID:** DiameterAppAnswerTaskQueueUtilization  
**Recovery:**

1. Application Routing might be misconfigured and is sending too much traffic to the Diameter Application. Verify the configuration by selecting **Diameter > Maintenance > Application Routing Rules** in the SO GUI.

2. If no additional congestion alarms are asserted, the Diameter Application Task might be experiencing a problem that is preventing it from processing messages from its Answer Message Queue. Examine the Alarm log in **Alarms & Events**.

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

### 13409 - Diameter Application Ingress Message Rate Exceeded

**Alarm Type:** UDRF  
**Description:** This alarm is raised from an MP based on the ingress and routing message rate thresholds listed on the **Diameter Common > MPs > Profiles** page. The specific parameters that correspond to this alarm are RxSprfemsgRateMinorSet, RxSprfemsgRateMinorClear, RxSprfemsgRateMajorSet, RxSprfemsgRateMajorClear, RxSprfemsgRateCriticalSet, RxSprfemsgRateCriticalClear. This alarm is raised and cleared by individual MPs.

The alarm severity depends upon the amount of the Notification Table being used:
• Minor when utilization exceeds 80%.
• Major when utilization exceeds 90%.
• Critical when utilization exceeds 100%.

Severity: Major (Minor, Critical)
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: DiameterAppIngressMessageRateExceeded

Recovery:
1. Application Routing might be misconfigured and is sending too much traffic to the Diameter Application. Verify the configuration by selecting Diameter > Configuration > Application Route Tables 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).

13410 - UDR Process CPU Utilization Threshold Exceeded

Alarm Type: UDR

Description: The UDR Process CPU Utilization is approaching its maximum capacity. The alarm severity depends on the amount of CPU being used:

• Minor when utilization exceeds 60%.
• Major when utilization exceeds 66%.
• Critical when utilization exceeds 72%.

Severity: Minor (Major, Critical)
Instance: N/A
HA Score: Normal
Auto Clear Seconds: 0
OID: UdrbeProcCpuThresh

Recovery:
1. Reduce the traffic rate to clear the alarm. The alarm clears when utilization falls below these thresholds:
   • <= 57% (clears Minor alarm)
   • <= 63% (clears Major alarm)
   • <= 69% (clears Critical alarm)
2. If the problem persists, contact My Oracle Support (MOS).
13451 - Message Decoding Failure

Alarm Type: UDRF

Description: Message received was rejected because of a decoding failure. Decoding Failures can include: bad message/parameter length received; answer decode failure; diameter AVP not present; AVP occurs too many times in a Diameter message.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

 OID: SprfeMessageDecodingFailure

Recovery:

1. Determine the cause of the decoding failure and resend the message.
2. If the problem persists, contact My Oracle Support (MOS).

13452 - Unknown Command Code

Alarm Type: UDRF

Description: Either the message could not be routed because the Diameter Command Code in the ingress Request message is not supported (the Diameter Command Code is not UDR, PUR or SNR); or the response could not be sent because the Diameter Command Code in the response message is not supported (the Diameter Command Code is not PNA).

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

 OID: SprfeUnknownCommandCode

Recovery:

1. Resolve the command code and resend the message.
2. If the problem persists, contact My Oracle Support (MOS).

13453 - ComAgent Error

Alarm Type: UDRF

Description: This event occurs when the UDRFE application receives a ComAgent Error (timeout, congestion, or queue full) for the sent SprEvent. This event is raised when:

1) UDRFE fails to send a notifyAck event to ComAgent
2) UDRFE fails to send a UDR message to ComAgent
3) An internal client error or internal server error occurs
4) A timeout, congestion, or queue full error occurs

**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** N/A  
**OID:** SprfeDbConnectionError

**Recovery:**

1. Verify that the ComAgent connection status between UDR and UDRBE is up.
2. If the connection is not up or is degraded, restart the UDR process on MP and the UDRBE process on NO.
   a) At the command line on the MP server, enter `pm.set off udr` (to stop process).
   b) At the command line on the MP server, enter `pm.set on udr` (to restart process).
   c) At the command line on the NO server, enter `pm.set off udrbe` (to stop process).
   d) At the command line on the NO server, enter `pm.set on udrbe` (to restart process).
3. If necessary, slow down the traffic rate to bring back the connection state to Available.
4. If the problem persists, contact *My Oracle Support (MOS)*.

**13456 - Invalid Service Indication**

**Alarm Type:** UDRF  
**Description:** Message received from a peer that was rejected because no register ID could be mapped because the service indication received in the request is not supported by ESPR application (RegisterID not found for a service Indication).

**Severity:** Info  
**Instance:** N/A  
**HA Score:** Normal  
**Auto Clear Seconds:** N/A  
**OID:** SprfeInvalidServiceIndication

**Recovery:**

1. Fix the service indication and resend the message.
2. If the problem persists, contact *My Oracle Support (MOS)*.

**13457 - Orphan Response Event Received from UDRBE**

**Alarm Type:** UDRF  
**Description:** A response event was received from UDRBE for which no pending request transaction existed, resulting in the response event being discarded.

**Severity:** Info  
**Instance:** N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: SprfeOrphanResponseEventRcvdFromUdrbe
Recovery:
   No action required.

13458 - Orphan Response Event Received from peer
Alarm Type: UDRF
Description: An Answer message was received from a peer for whom no pending request transaction existed, resulting in the Answer message being discarded.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: SprfeOrphanResponseRcvdFromPeer
Recovery:
   No action required.

13459 - Sending Client Invalid
Alarm Type: UDRF
Description: This event is generated each time a client sends a request that it is not permitted to send. This could be because:
   • The client was not present in the Subscribing Client Permissions table.
   • The client was present in the Subscribing Client Permissions table, but was not authorized to send the Sh Operation (PUR, SNR or UDR).
   • The DataReference value supplied was not 0 (i.e. RepositoryData).
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: SprfeSendingClientInvalid
Recovery:
   1. Determine the issue and resend the request.
   2. If the problem persists, contact My Oracle Support (MOS).
13460 - Client Not Subscribed

Alarm Type: UDRF

Description: This event is generated each time a PNR is sent to an AS, and the AS responds with a PNA, indicating that it was not subscribed to receive notifications for the subscriber to which it was notified.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: SprfeClientNotSubscribed

Recovery:
1. Subscribe the application server to received notifications and resend the PNR.
2. If the problem persists, contact My Oracle Support (MOS).

13461 - Invalid Parameter Value

Alarm Type: UDRF

Description: This event is generated each time an AS sends PUR, SNR, or UDR that contains a parameter that fails application validation. Validation failures include:

- Diameter AVP value is invalid.
- The requested operation is not allowed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: SprfeInvalidParameterValue

Recovery:
1. Determine why the application failed validation and resend the request.
2. If the problem persists, contact My Oracle Support (MOS).

13462 - PNR Create Failed

Alarm Type: UDRF

Description: This event is generated each time a PNR request fails to be created or the origin host/realm or destination host/realm could not be determined.

Severity: Info

Instance: N/A

HA Score: Normal
Auto Clear Seconds: N/A
OID: SprfePnrCreateFailed
Recovery:
   No action required.

13463 - Diameter Application Enabled
Alarm Type: UDRF
Description: This event is generated when Diameter's Application Admin State variable is changed to enabled.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: DiameterAppEnabled
Recovery:
   No action required.

13464 - Diameter Application Disabled
Alarm Type: UDRF
Description: This event is generated when Diameter's Application Admin State variable is changed to disabled.
Severity: Info
Instance: N/A
HA Score: Normal
Auto Clear Seconds: N/A
OID: DiameterAppDisabled
Recovery:
   No action required.

19800-19899 - Communication Agent
This section provides information and recovery procedures for Communication Agent (ComAgent) alarms and events, ranging from 19800 - 19899, 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 ingress 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:** The Communication Agent egress message is being discarded due to one of the following reasons:

- Unknown destination server
- Connection state is not InService
- Incompatible destination
- Serialization failed
- MxEndpoint send failed
- Internal error

**Severity:** Info

**Instance:** <RemoteIP>

**Note:** If <RemoteIP> is not known at the time of message discard, then "Unknown" will be used.

**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
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
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
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
Auto Clear Seconds: 0 (zero)
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 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 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.

**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
Alarms and Events

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
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
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>`

- 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
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
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
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

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
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
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  
**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

**Alarm Type:** CAF  
**Description:** The Communication Agent service provider registration state changed.  
**Severity:** Info
Instance: <ServiceName>
HA Score: Normal
Auto Clear Seconds: 0
OID: cAFEventSvcProvRegStateChangedNotify
Recovery:
   No action required.

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
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 (30 minutes)
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:** 10

**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
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
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: <PeerGroupName>
HA Score: Normal
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: <PeerGroupName>
HA Score: Normal
Throttle Seconds: 10
OID: cAFEventPSEgressMessageDiscardedNotify
Recovery:
Generally, this alarm is informational and no action is required.

19868 - Communication Agent Connection Rejected - Incompatible Network

Event Type: CAF
Description: Communication Agent connection rejected. Connection to the peer node is not initiated due to network incompatibility. This event will be raised on the connection initiator side when the connection initiator MP has only IPv6 IP addresses configured and Remote MP has only IPv4 IP addresses configured or when connection initiator MP has only IPv4 IP addresses configured and Remote MP has only IPv6 IP addresses configured.
Severity: Info
Instance: <RemoteIP>
HA Score: Normal
OID: cAFEventConnectionRejectNotify
Recovery:
1. Disable both sides of the connection.
2. Configure the correct network modes on either server.
3. Restart the application on the reconfigured server.
4. Enable both sides of the connection.
5. Contact My Oracle Support (MOS) for assistance if needed.
19900-19999 - EXG Stack

This section provides information and recovery procedures for EXG Stack alarms, ranging from 19900-19999.

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.

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.

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
Auto Clear Seconds: 120
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.

22000-22999 - Diameter

This section provides information and recovery procedures for Diameter alarms and events, ranging
from 22000 - 22999, 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.

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.
- Severity: Info
- Instance: <TransConnName>
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>

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>

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:
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 Route Tables 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
Note: Because many route lists can be created on a DA-MP server, care must be taken to prevent excessive event generation with these resources.
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 Config Set specified 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

Note: Because many route lists can be created on a DA-MP server, care must be taken to prevent excessive event generation with these resources.

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:** &lt;NetworkElement&gt;

**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:** &lt;NetworkElement&gt;

**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 configured size limit

Event Type: DIAM
Description: The generated Copy message size exceeded the max message size on the system.
Severity: Info
Alarms and Events

Instance: <DA-MP>
HA Score: Normal
Throttle Seconds: 10

Note: Because many copy messages can exceed the system configured size, care must be taken to prevent excessive generation with these resources.

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

Alarm Group: DIAM
Description: Debug Routing Info AVP is enabled.
Severity: Minor
Instance: None
HA Score: Normal
Auto Clear Seconds: 0 (zero)
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:* &lt;ETGName&gt;  
*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:* &lt;ETGName&gt;  
*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: Info

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 a 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: Info

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: Info
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.

22064 - Upon receiving Redirect Host Notification the Request has not been submitted for re-routing
Event Type: DIAM
Description: This event indicates that the DSR has encountered a Redirect Host Notification that it can accept for processing but cannot continue processing due to some reason, such as internal resources exhaustion.
Severity: Info
Instance: <PeerName>
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterRxRedirectHostNotRoutedNotify
Recovery:
1. Examine the DA-MP congestion status and related measurements and take appropriate action.
2. If the problem persists, contact My Oracle Support (MOS)

22065 - Upon receiving Redirect Realm Notification the Request has not been submitted for re-routing
Event Type: DIAM
Description: The Redirect Realm Notification received is accepted but cannot be processed due to some reason, such as internal resources exhaustion.
Severity: Info
Instance: <PeerName>
HA Score: Normal
Throttle Seconds: 60
OID: eagleXgDiameterRxRedirectRealmNotRoutedNotify

Recovery:
1. Examine the DA-MP congestion status and related measurements and take appropriate action.
2. If the problem persists, contact My Oracle Support (MOS)

22066 - ETG-ETL Scope Inconsistency

Event Type: DIAM
Description: An ETG's Control Scope is set to ETL, but the ETG is not configured against an ETL.
Severity: Minor
Instance: <ETG Name>
HA Score: Normal
Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgEtlscopeInconsistencyNotify

Recovery:
1. Correct the configuration inconsistency by changing the Control Scope of the ETG from ETL to ETG, or by adding the ETG to an ETL.
2. If a backup image has been restored to the SOAM, but not the NOAM, restoring a consistent backup image for the NOAM should resolve the problem.
3. If the problem persists, contact My Oracle Support (MOS).

22067 - ETL-ETG Invalid Association

Event Type: DIAM
Description: An ETL is associated with an ETG that does not exist.
Severity: Minor
Instance: <ETL Name>
HA Score: Normal
Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgEtlInvalidAssocNotify

Recovery:
1. Correct the configuration inconsistency by updating the ETL to refer to a valid ETG, or by installing consistent backups on the NOAM and SOAM.
2. If the problem persists, contact My Oracle Support (MOS).

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.
- **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.
Alarms and Events

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 DA-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. Reduce traffic to the MP.

2. Verify that no network issues exist between the DA-MP and the intended DAS peer(s).

3. Verify that the intended DAS peer has sufficient capacity to process the traffic load being routed to it.

4. 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
Alarms and Events

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. The alarm severity depends on the amount of MP CPU being used:
- Minor when MP utilization is equal to or greater than 80%
- Major when MP utilization is equal to or greater than 90%
- Critical when MP utilization equals 100%

**Severity:** Major (Minor, 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
Alarms and Events

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 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.
2. 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 from Event Addn'l Data 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 errno value and text from Event Addn'l Info 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.
2. If the problem persists, contact My Oracle Support (MOS).

22315 - Connection Unavailable: Peer IP address validation failure
Event Type: DIAM
Description: Actual peer connection IP address does not match configured peer IP address.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailPeerIpAddrVldtnFailNotify
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).
22317 - Connection Rejected: Connection already established

Event Type: DIAM
Description: Peer initiated connection was rejected because locally initiated connection has already completed capabilities exchange.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterConnRejectedConnAlrdyEstdNotify
Recovery:
1. If condition persists, diagnose peer to determine reason for the second connection initiation.
2. If the problem persists, contact My Oracle Support (MOS).

22318 - Connection Rejected: Connection not Enabled

Event Type: DIAM
Description: Peer initiated connection was rejected because connection was locally Admin Disabled.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 30
OID: eagleXgDiameterConnRejectedConnNotEnabledNotify
Recovery:
1. Resolve inconsistency between the local and peer nodes Administrative State.
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 DA-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).

22324 - Connection Unavailable: CER validation failure

Event Type: DIAM
Description: CER contained invalid or unsupported AVP or AVP value.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Throttle Seconds: 1
OID: eagleXgDiameterConnUnavailCerValidationFailureNotify
Recovery:
1. Disable peer’s use of inband security.
2. If the problem persists, contact *My Oracle Support (MOS)*.

### 22325 - Host-IP-Address AVP(s) in CER/CEA do not match peer IP address(es)

**Event Type:** DIAM  
**Description:** The Host-IP-Address AVP(s) received in a CER or CEA message from the peer did not match the actual peer connection’s IP address(es).  
**Severity:** Info  
**Instance:** `<TransConnName>`  
**HA Score:** Normal  
**Throttle Seconds:** 1  
**OID:** eagleXgDiameterConnUnavilCerHostIpAvpVldtnFailNotify  
**Recovery:**  
1. Diagnose peer to resolve inconsistency.  
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.

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.
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)*.

**22333 - Connection Rejected: Insufficient Ingress MPS**

**Event Type:** DIAM  
**Description:** Connection was rejected due to insufficient Ingress MPS on the DA-MP to support the Reserved Ingress MPS configured for the connection. This sum of the Reserved Ingress MPS for the added connection and MP Reserved Ingress MPS has exceeded the MP Maximum Reserved Ingress MPS.
**Severity:** Info

**Instance:** <TransConnName>

**HA Score:** Normal

**Throttle Seconds:** 10

**OID:** eagleXgDiameterConnRejInsufficientIngressMpsNotify

**Recovery:**

1. The value for Reserved Ingress MPS for the added connection needs to be examined to determine if its value should be decreased.
2. Contact *My Oracle Support (MOS)* for assistance.

**22334 - Unexpected Message Priority in ingress Request**

**Event Type:** DIAM  
**Description:** The Priority value decoded from the incoming message is not correct.  
**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:** The Peer does not support the Message Priority feature. Therefore, the Peer does not encode Message Priority in the request.  
**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”.

22336 - Connection Rejected: Multihomed SCTP connection attempt

Event Type: DIAM
Description: Connection was rejected because the peer attempted to initiate an SCTP multihomed connection to an IPFE connection.
Severity: Info
Instance: <TransConnName>
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: eagleXgDiameterConnRejMHsctpConnAttemptNotify
Recovery:
1. Update the peer to initiate unihomed IPFE SCTP connections.
2. Contact My Oracle Support (MOS) for assistance.

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 DSR message processor is Unavailable or Congested.
Severity: Info
Instance: <SourceMpHost>
HA Score: Normal
Throttle Seconds: 10
OID: eagleXgDiameterProcessorUnavlblOrCngstedNotify
Recovery:
1. See the recovery steps for measurement RxAnsFwdFailed in DSR Measurement Reference.
2. 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 - DA-MP Reserved Ingress MPS Oversubscribed

Event Type: DIAM
Description: The total connection Reserved Ingress MPS exceeds the Engineered Ingress MPS capacity of the DA-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: Major, Critical
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: Major, Critical

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
Alarms and Events

**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**: `<DbTblName>` (Name of the Diameter Connection Status Sharing Table where the Diameter Connection status inconsistency was 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).

25000-25499 - Computer Aided Policy Making

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 - CAPM Update Failed

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 - CAPM Action Failed

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 - CAPM Exit Rule Template

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>
25003 - CAPM Exit Trigger

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: eagleXgDiameterCapmExitRuleFailedNotify

Recovery: No action required.

25004 - Script failed to load

Alarm Type: CAPM

Description: Script syntax error

Severity: Minor

Instance: <script name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterCapmScriptLoadingFailedNotify

Recovery:

Check for syntax errors in the script

25005 - CAPM Generic Event

Event Type: CAPM

Description: CAPM Generic Event

Severity: Info

Instance: <template-id:rule-id>
25006 - CAPM Generic Alarm - Minor
Event Type: CAPM
Description: CAPM Generic Alarm - Minor
Severity: Minor
Instance: <template-id:rule-id>
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDiameterCapmGenericMinorAlarmNotify
Recovery:
   Contact My Oracle Support (MOS).

25007 - CAPM Generic Alarm - Major
Event Type: CAPM
Description: CAPM Generic Alarm - Major
Severity: Major
Instance: <template-id:rule-id>
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDiameterCapmGenericMajorAlarmNotify
Recovery:
   Contact My Oracle Support (MOS).

25008 - CAPM Generic Alarm - Critical
Event Type: CAPM
Description: CAPM Generic Alarm - Critical
Severity: Critical
Instance: <template-id:rule-id>
HA Score: Normal
Auto Clear Seconds: 300
OID: eagleXgDiameterCapmGenericCriticalAlarmNotify
Recovery:
   Contact My Oracle Support (MOS).

25500-25899 - OAM Alarm Management

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: eagleXgDiameterNoDaMpLeader DetectedNotify
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: eagleXgDiameterMultipleDaMpLeaderDetectedNotify
Recovery:
   If the problem persists, contact My Oracle Support (MOS) for assistance.
31000-32700 - Platform

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32700. Platform provides basic functionality that is shared across products.

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.

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
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 IMU 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
31118 - Database disk store fault

**Alarm Group:** DISK

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

**Severity:** Minor

**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

**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 PeriodDB Ousted Throttle Behind
Alarm Group: DB
Description: IDB has one or more processes throttled for an extended period. DB ousted throttle may be affecting processes.
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolOustedThrottleWarnNotify

Recovery:
1. Monitor for workload in excess of documented capacity. Run `procshm -o` to identify involved processes.
2. Contact *My Oracle Support (MOS)* if this alarm persists.

### 31140 - Database perl fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbPerlFaultNotify

Recovery:

Contact *My Oracle Support (MOS).*

### 31145 - Database SQL fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbSQLFaultNotify

Recovery:

1. Export event history for the given server, and `Imysqld` task.
2. Contact *My Oracle Support (MOS).*
31146 - DB mastership fault

Alarm Group: SW

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMastershipFaultNotify

Recovery:
1. Export event history for the given server.
2. Contact *My Oracle Support (MOS)*.

31147 - DB upsynclog overrun

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpSyncLogOverrunNotify

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

31148 - DB lock error detected

Alarm Group: DB

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbLockErrorNotify
Recovery:

Contact My Oracle Support (MOS).

31200 - Process management fault
Alarm Group: SW
Description: The process manager (procmgr) is impaired by a s/w fault
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolProcMgmtFaultNotify
Recovery:
1. Export event history for the given server, all processes.
2. Contact My Oracle Support (MOS).

31201 - Process not running
Alarm Group: PROC
Description: A managed process cannot be started or has unexpectedly terminated
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolProcNotRunningNotify
Recovery:

Contact My Oracle Support (MOS).

31202 - Unkillable zombie process
Alarm Group: PROC
Description: A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolProcZombieProcessNotify
Recovery:
1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. Contact My Oracle Support (MOS).

31206 - Process mgmt monitoring fault
Alarm Group: SW
Description: The process manager monitor (pm.watchdog) is impaired by a s/w fault
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolProcMgmtMonFaultNotify
Recovery:
   Contact My Oracle Support (MOS).

31207 - Process resource monitoring fault
Alarm Group: SW
Description: The process resource monitor (ProcWatch) is impaired by a s/w fault
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolProcResourceMonFaultNotify
Recovery:
   Contact My Oracle Support (MOS).

31208 - IP port server fault
Alarm Group: SW
Description: The run environment port mapper (re.portmap) is impaired by a s/w fault
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
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

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

Recovery:
Contact My Oracle Support (MOS).

31214 - Scheduled process fault

Alarm Group: PROC
Description: A scheduled process cannot be executed or abnormally terminated
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolScheduleProcessFaultNotify

Recovery:
  Contact My Oracle Support (MOS).

31215 - Process resources exceeded

Alarm Group: SW

Description: A process is consuming excessive system resources

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 14400

OID: comcolProcResourcesExceededFaultNotify

Recovery:
  Contact My Oracle Support (MOS).

31216 - SysMetric configuration error

Alarm Group: SW

Description: A SysMetric Configuration table contains invalid data

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSysMetricConfigErrorNotify

Recovery:
  Contact My Oracle Support (MOS).

31220 - HA configuration monitor fault

Alarm Group: SW

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

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaCfgMonitorFaultNotify

Recovery:
   Contact My Oracle Support (MOS).

31221 - HA alarm monitor fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAlarmMonitorFaultNotify

Recovery:
   Contact My Oracle Support (MOS).

31222 - HA not configured

Alarm Group: HA

Description: High availability is disabled due to system configuration

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaNotConfiguredNotify

Recovery:
   Contact My Oracle Support (MOS).

31223 - HA Heartbeat transmit failure

Alarm Group: HA
Description: The high availability monitor failed to send heartbeat
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaHbTransmitFailureNotify
Recovery:
1. This alarm clears automatically when the server successfully registers for HA heartbeating.
2. If this alarm does not clear after a couple minutes, contact My Oracle Support (MOS).

31224 - HA configuration error
Alarm Group: HA
Description: High availability configuration error
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaCfgErrorNotify
Recovery:

Contact My Oracle Support (MOS).

31225 - HA service start failure
Alarm Group: HA
Description: The required high availability serviceresource 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 measurements collector (statclerk) is impaired by a s/w fault
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolMeasCollectorFaultNotify
Recovery:
1. Export event history for the given server and statclerk task.
2. Contact *My Oracle Support (MOS)*.

31250 - RE port mapping fault
Alarm Group: SW
Description: The IP service port mapper (re.portmap) is impaired by a s/w fault
Severity: Minor
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolRePortMappingFaultNotify

Recovery:
This typically 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: DbcomcolSnmpAgentNotify
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
31294 - HA Resource Status

Alarm Group: HA
Description: HA Resource registration status
Severity: Info

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

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.

31301 - HA Topology Events

Alarm Group: HA
Description: HA topology events
Severity: Info
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 300
OID: comcolHaTopologyNotify
Recovery:
   Status message - no action required.
### 32113 - Uncorrectable ECC memory error

**Alarm Group:** PLAT  
**Description:** This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.  
**Severity:** Critical  
**Instance:** May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr  
**HA Score:** Normal  
**Auto Clear Seconds:** 0 (zero)  
**OID:** tpdEccUncorrectableError  
**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:
1. 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**

1. Determine if the hardware platform is PP5160.

   **Note:** SDM on the PP5160 platform uses raid0 configuration.

   If the platform is a PP5160, no action is required.

2. 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).

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 lower right port on the rear of the server.port of the quad-port card in PCI slot 9.to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.
2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.
4. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, contact My Oracle Support (MOS).
32312 - Server disk space shortage error

**Alarm Group:** PLAT

**Description:** This alarm indicates that one of the following conditions has occurred:
- A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system.
- More than 90% of the total number of available files have been allocated on the file system.
- A file system has a different number of blocks than it had when installed.

**Severity:** Major

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

**HA Score:** Normal

**Auto Clear Seconds:** 0 (zero)

**OID:** tpdDiskSpaceShortageError

**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:** 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).

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 both servers/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 15: 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 15: 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 16: 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 both 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 heartbeat is running (service TKLCha status).
   - Note: This step may require command line ability.


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).
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).*

32337 - Flash Program Failure

**Alarm Group:** PLAT

**Description:** This alarm indicates that there was an error while trying to update the firmware flash on the E5-APP-B cards.

**Severity:** Major

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

**HA Score:** Normal
Auto Clear Seconds: 0 (zero)
OID: tpdFlashProgramFailure
Recovery
   Contact My Oracle Support (MOS).

32338 - Serial Mezzanine Unseated
Alarm Group: PLAT
Description: This alarm indicates that a connection to the serial mezzanine board may not be properly seated.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdSerialMezzUnseated
Recovery
   1. Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.
   2. Contact My Oracle Support (MOS) if reseating the cables does not clear the alarm.

32339 - Max pid limit
Alarm Group: PLAT
Description: This alarm indicates that the maximum number of running processes has reached the major threshold.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdMaxPidLimit
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)

32348 - FIPS subsystem problem
Alarm Group: PLAT
Description: This alarm indicates the FIPS subsystem is not running or has encountered errors.
Severity: Major
Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr
HA Score: Normal
Auto Clear Seconds: 0 (zero)
OID: tpdFipsSubsystemProblem

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

32349 - File Tampering

Alarm Group: PLAT

Description: This alarm indicates HIDS has detected file tampering.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdHidsFileTampering

Recovery

Contact My Oracle Support (MOS).

32350 - Security Process Terminated

Alarm Group: PLAT

Description: This alarm indicates that the security process monitor is not running.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSecurityProcessDown

Recovery

Contact My Oracle Support (MOS).

32500 – Server disk space shortage warning

Alarm Group: PLAT

Description: 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).
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.

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDefaultRouteNotDefined

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. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the room returns to an acceptable temperature before syscheck shows 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. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

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**


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)](http://www.oracle.com) 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.

### 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  
**Throttle Seconds:** 86400  
**OID:** tpdTelcoSwitchNotification  

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

### 32701 - HIDS Initialized

**Alarm Type:** PLAT  
**Description:** This alarm indicates HIDS was initialized.  
**Default Severity:** Info  
**OID:** tpdHidsBaselineCreated  

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

### 32702 - HIDS Baseline Deleted

**Alarm Type:** PLAT  
**Description:** HIDS baseline deleted  
**Default Severity:** Info  
**OID:** tpdHidsBaselineDeleted  

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

### 32703 - HIDS Enabled

**Alarm Type:** PLAT  
**Description:** HIDS Enabled  
**Default Severity:** Info  
**OID:** tpdHidsEnabled
Recovery
   Contact My Oracle Support (MOS).

32704 - HIDS Disabled
Alarm Type: PLAT
Description: HIDS disabled
Default Severity: Info
OID: tpdHidsDisabled
Recovery
   Contact My Oracle Support (MOS).

32705 - HIDS Monitoring Suspended
Alarm Type: PLAT
Description: HIDS monitoring suspended
Default Severity: Info
OID: tpdHidsSuspended
Recovery
   Contact My Oracle Support (MOS).

32706 - HIDS Monitoring Resumed
Alarm Type: PLAT
Description: HIDS monitoring resumed
Default Severity: Info
OID: tpdHidsResumed
Recovery
   Contact My Oracle Support (MOS).

32707 - HIDS Baseline Updated
Alarm Type: PLAT
Description: HIDS baseline updated
Default Severity: Info
OID: tpdHidsBaselineUpdated
Recovery
   Contact My Oracle Support (MOS).
Chapter 4

Key Performance Indicators (KPIs)

This section provides general information about KPIs, and lists the KPIs that can appear on the Status & Manage KPIs GUI page.

Topics:

- General KPIs information.....261
- List of KPIs.....263
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 N/A.

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 NOAM server or an SOAM server.

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 NOAM server or an SOAM server. Collection of KPI data is handled solely by NOAM servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the KPIs Export page.
### 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 transferred to an

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Frequency</td>
<td>Frequency at which the export occurs</td>
<td>Format: Radio button&lt;br&gt;Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily&lt;br&gt;Default: Once</td>
</tr>
<tr>
<td>Task Name</td>
<td>Name of the scheduled task</td>
<td>Format: Textbox&lt;br&gt;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.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the scheduled task</td>
<td>Format: Textbox&lt;br&gt;Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.</td>
</tr>
<tr>
<td>Minute</td>
<td>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.</td>
<td>Format: Scrolling list&lt;br&gt;Range: 0 to 59&lt;br&gt;Default: 0</td>
</tr>
<tr>
<td>Time of Day</td>
<td>Time of day the export occurs</td>
<td>Format: Time textbox&lt;br&gt;Range: 15-minute increments&lt;br&gt;Default: 12:00 AM</td>
</tr>
<tr>
<td>Day of Week</td>
<td>Day of week on which the export occurs</td>
<td>Format: Radio button&lt;br&gt;Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday&lt;br&gt;Default: Sunday</td>
</tr>
</tbody>
</table>
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** 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*

---

### List of KPIs

This section of the document provides a list of all KPIs that can appear on the KPI page. They are listed here in tables by KPI type.

### KPIs server elements

This table describes KPIs that appear regardless of server role.
Table 18: KPIs Server Elements

<table>
<thead>
<tr>
<th>KPIs Status Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Element</td>
<td>The network element name (set up on the Configuration &gt; Network Elements page) associated with each Server Hostname.</td>
</tr>
<tr>
<td>Server Hostname</td>
<td>The server hostname set up on the Configuration &gt; Servers page. All servers in the system are listed here.</td>
</tr>
</tbody>
</table>

Server Indicators:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Percentage utilization of all processors on the server by all software as measured by the operating system.</td>
</tr>
<tr>
<td>RAM</td>
<td>Percentage utilization of physical memory on the server by all software as measured by TPD.</td>
</tr>
<tr>
<td>Swap</td>
<td>Percentage utilization of swap space on the server by all software as measured by TPD.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The total amount of time the server has been running.</td>
</tr>
</tbody>
</table>

Process-based KPIs

Table 19: Process-based KPIs

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>udr.Cpu</td>
<td>CPU usage of udr process</td>
</tr>
<tr>
<td>udr.MemHeap</td>
<td>Heap memory usage of udr process</td>
</tr>
<tr>
<td>udr.MemBasTotal</td>
<td>Memory usage of the udr process</td>
</tr>
<tr>
<td>udr.MemPerTotal</td>
<td>Percent memory usage of udr process</td>
</tr>
<tr>
<td>udrbe.Cpu</td>
<td>CPU usage of udrbe process</td>
</tr>
<tr>
<td>udrbe.MemHeap</td>
<td>Heap memory usage of udrbe process</td>
</tr>
<tr>
<td>udrbe.MemBasTotal</td>
<td>Memory usage of the udrbe process</td>
</tr>
<tr>
<td>udrbe.MemPerTotal</td>
<td>Percent memory usage of udrbe process</td>
</tr>
<tr>
<td>provimport.Cpu</td>
<td>CPU usage of provimport process</td>
</tr>
<tr>
<td>provimport.MemHeap</td>
<td>Heap memory usage of provimport process</td>
</tr>
<tr>
<td>provimport.MemBasTotal</td>
<td>Memory usage of the provimport process</td>
</tr>
<tr>
<td>provimport.MemPerTotal</td>
<td>Percent memory usage of provimport process</td>
</tr>
<tr>
<td>provexport.Cpu</td>
<td>CPU usage of provexport process</td>
</tr>
</tbody>
</table>
### Key Performance Indicators (KPIs)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>provexport.MemHeap</td>
<td>Heap memory usage of provexport process</td>
</tr>
<tr>
<td>provexport.MemBasTotal</td>
<td>Memory usage of the provexport process</td>
</tr>
<tr>
<td>provexport.MemPerTotal</td>
<td>Percent memory usage of provexport process</td>
</tr>
<tr>
<td>udrprov.Cpu</td>
<td>CPU usage of ras process</td>
</tr>
<tr>
<td>udrprov.MemHeap</td>
<td>Heap memory usage of ras process</td>
</tr>
<tr>
<td>udrprov.MemBasTotal</td>
<td>Memory usage of the ras process</td>
</tr>
<tr>
<td>udrprov.MemPerTotal</td>
<td>Percent memory usage of ras process</td>
</tr>
<tr>
<td>udrprov.Cpu</td>
<td>CPU usage of xsas process</td>
</tr>
<tr>
<td>udrprov.MemHeap</td>
<td>Heap memory usage of xsas process</td>
</tr>
<tr>
<td>udrprov.MemBasTotal</td>
<td>Memory usage of the xsas process</td>
</tr>
<tr>
<td>udrprov.MemPerTotal</td>
<td>Percent memory usage of xsas process</td>
</tr>
<tr>
<td>era.Cpu</td>
<td>CPU usage of era process</td>
</tr>
<tr>
<td>era.MemHeap</td>
<td>Heap memory usage of era process</td>
</tr>
<tr>
<td>era.MemBasTotal</td>
<td>Memory usage of the era process</td>
</tr>
<tr>
<td>era.MemPerTotal</td>
<td>Percent memory usage of era process</td>
</tr>
</tbody>
</table>

### UDRBE KPIs

**Table 20: UDRBE KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxAeProvCreateMsgsRate</td>
<td>Number of requests received via the provisioning interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber per second</td>
</tr>
<tr>
<td>RxAeProvCreateSubSuccessRate</td>
<td>Number of auto-enrolled subscribers created while provisioning non-profile entity data per second</td>
</tr>
<tr>
<td>RxAeShCreateSubSuccessRate</td>
<td>Number of auto-enrolled subscribers created via the Sh interface per second</td>
</tr>
<tr>
<td>RxAeShDeleteSubMsgs</td>
<td>Number of unsubscribe requests received via the Sh interface that triggered the removal of an auto-enrolled subscriber per second</td>
</tr>
<tr>
<td>RxAeShDeleteSubSuccess</td>
<td>Number of auto-enrolled subscribers deleted via the Sh interface per second</td>
</tr>
<tr>
<td>RxAeShPurCreateMsgsRate</td>
<td>Number of update requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber per second</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>RxAeShSnrcCreateMsgsRate</td>
<td>Number of subscribe requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber per second</td>
</tr>
<tr>
<td>RxUdrBeReadMsgsRate</td>
<td>Number of read requests (across all interfaces) that have been received per second</td>
</tr>
<tr>
<td>RxUdrBeUpdateMsgsRate</td>
<td>Number of update requests (across all interfaces) that have been received per second</td>
</tr>
<tr>
<td>RxUdrNmNotifAckAsAvailableRate</td>
<td>Number of notification requests (across all interfaces) that have been successfully sent to the AS per second</td>
</tr>
<tr>
<td>RxUdrNmNotifAckAsUnavailableRate</td>
<td>Number of notification requests (across all interfaces) that failed to be sent to the AS per second</td>
</tr>
<tr>
<td>RxUdrSmSubscribeMsgsRate</td>
<td>Number of subscribe requests (across all interfaces) that have been received per second</td>
</tr>
<tr>
<td>RxUdrSmUnsubscribeMsgsRate</td>
<td>Number of unsubscribe requests (across all interfaces) that have been received per second</td>
</tr>
<tr>
<td>SQRQuotaRowElementsResetRate</td>
<td>Number of Quota Row Elements currently being reset or updated</td>
</tr>
<tr>
<td>SQRRecordsExaminedRate</td>
<td>Number of Subscriber/Pool Records currently being examined</td>
</tr>
<tr>
<td>SQRRecordsFailedRate</td>
<td>Number of Subscriber/Pool Records currently failed to reset or updated</td>
</tr>
<tr>
<td>SQRRecordsResetRate</td>
<td>Number of Subscriber/Pool Records currently being reset or updated</td>
</tr>
<tr>
<td>TxUdrBeReadReqSuccessRate</td>
<td>The number of read requests (across all interfaces) that have been successfully processed per second</td>
</tr>
<tr>
<td>TxUdrBeUpdateReqSuccessRate</td>
<td>The number of update requests (across all interfaces) that have been successfully processed per second</td>
</tr>
<tr>
<td>TxUdrNmNotifSentRate</td>
<td>The number of notification requests (across all interfaces) that have been sent per second</td>
</tr>
<tr>
<td>TxUdrSmSubscribeReqSuccessRate</td>
<td>The number of subscribe requests (across all interfaces) that have been successfully processed per second</td>
</tr>
<tr>
<td>TxUdrSmUnsubscribeReqSuccessRate</td>
<td>The number of unsubscribe requests (across all interfaces) that have been successfully processed per second</td>
</tr>
</tbody>
</table>
### UDRFE KPIs

**Table 21: UDRFE KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRequestAllRate</td>
<td>The number of signaling requests that have been received per second.</td>
</tr>
<tr>
<td>RxRequestFailedRate</td>
<td>The number of signaling requests that have failed to be processed due to errors and an error was returned per second.</td>
</tr>
<tr>
<td>RxRequestSuccessfulRate</td>
<td>The number of signaling requests that have been successfully processed and a Diameter Successful response (2001) was received per second.</td>
</tr>
<tr>
<td>RxResetRequestPURFailedRate</td>
<td>Number of PUR Reset messages failed to process at this time</td>
</tr>
<tr>
<td>RxResetRequestPURRate</td>
<td>Number of PUR Reset messages received by OCUDR currently</td>
</tr>
<tr>
<td>RxResetRequestPURSuccessfulRate</td>
<td>Number of PUR Reset messages processed successfully at this time</td>
</tr>
<tr>
<td>RxResponseAllRate</td>
<td>The number of signaling responses that have been received per second.</td>
</tr>
<tr>
<td>TxRequestAllRate</td>
<td>The number of signaling requests sent per second</td>
</tr>
<tr>
<td>TxRequestFailedAllRate</td>
<td>The number of requests that have not received successful responses per second.</td>
</tr>
<tr>
<td>TxRequestSuccessfulAllRate</td>
<td>The number of requests that have received successful responses per second.</td>
</tr>
<tr>
<td>TxResponseAllRate</td>
<td>The number of signaling responses sent per second</td>
</tr>
</tbody>
</table>

### UDR RAS and XSAS Provisioning Related KPIs

**Table 22: Provisioning KPIs**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProvMsgsImportedRate</td>
<td>The number of provisioning messages imported per second</td>
</tr>
<tr>
<td>ProvTxnCommittedRate</td>
<td>The number of provisioning transactions that have been successfully committed per second to the database (memory and on disk) on the active server of the primary UDR cluster</td>
</tr>
<tr>
<td>RxRasDeleteReqReceivedRate</td>
<td>The number of REST DELETE requests that have been received on the provisioning interface per second</td>
</tr>
</tbody>
</table>
### Key Performance Indicators (KPIs)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxRasGetReqReceivedRate</td>
<td>The number of REST GET requests that have been received on the provisioning interface per sec</td>
</tr>
<tr>
<td>RxRasPostReqReceivedRate</td>
<td>The number of REST POST requests that have been received on the provisioning interface per sec</td>
</tr>
<tr>
<td>RxRasProvConnection</td>
<td>The number of provisioning client connections currently established. A single connection includes a client successfully establishing a TCP/IP connection, sending a provisioning connect message, and receiving a successful response.</td>
</tr>
<tr>
<td>RxRasProvMsgsReceivedRate</td>
<td>The number of provisioning messages that have been received per second</td>
</tr>
<tr>
<td>RxRasProvMsgsSuccessfulRate</td>
<td>The number of provisioning messages that have been successfully processed per second</td>
</tr>
<tr>
<td>RxRasProvMsgsFailedRate</td>
<td>The number of provisioning messages that have failed to be processed due to errors per second</td>
</tr>
<tr>
<td>RxRasProvMsgsSentRate</td>
<td>The number of provisioning messages sent per second</td>
</tr>
<tr>
<td>RxRasProvMsgsDiscardedRate</td>
<td>The number of provisioning messages discarded per second. Provisioning messages are discarded because the connection is shut down, the server is shut down, the server role switches from active to standby, or the transaction does not become durable within the allowed amount of time.</td>
</tr>
<tr>
<td>RxRasPutReqReceivedRate</td>
<td>The number of REST PUT requests that have been received on the provisioning interface per sec</td>
</tr>
<tr>
<td>RxXsasDeleteReqReceivedRate</td>
<td>The number of SOAP delete requests that have been received on the provisioning interface per sec</td>
</tr>
<tr>
<td>RxXsasInsertReqReceivedRate</td>
<td>The number of SOAP insert requests that have been received on the provisioning interface per sec</td>
</tr>
<tr>
<td>RxXsasOperationReqReceivedRate</td>
<td>The number of SOAP operation requests that have been received on the provisioning interface per sec</td>
</tr>
<tr>
<td>RxXsasProvConnection</td>
<td>The number of provisioning client connections currently established. A single connection includes a client having successfully established a TCP/IP connection, sent a provisioning connect message, and having received a successful response.</td>
</tr>
<tr>
<td>RxXsasProvMsgsReceivedRate</td>
<td>The number of provisioning messages that have been received per second</td>
</tr>
<tr>
<td>RxXsasProvMsgsSuccessfulRate</td>
<td>The number of provisioning messages that have been successfully processed per second</td>
</tr>
<tr>
<td>RxXsasProvMsgsFailedRate</td>
<td>The number of provisioning messages that have failed to be processed due to errors per second</td>
</tr>
</tbody>
</table>
## Key Performance Indicators (KPIs)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxXsasProvMsgsSentRate</td>
<td>The number of provisioning messages sent per second</td>
</tr>
<tr>
<td>RxXsasProvMsgsDiscardedRate</td>
<td>The number of provisioning messages discarded per second. Provisioning messages are discarded because the connection is shut down, the server is shut down, the server role switches from active to standby, or the transaction does not become durable within the allowed amount of time.</td>
</tr>
<tr>
<td>RxXsasProvTxnTotalRate</td>
<td>The number of provisioning SOAP transactions received per second</td>
</tr>
<tr>
<td>RxXsasSelectReqReceivedRate</td>
<td>The number of SOAP select requests that have been received on the provisioning interface per second</td>
</tr>
<tr>
<td>RxXsasUpdateReqReceivedRate</td>
<td>The number of SOAP update requests that have been received on the provisioning interface per second</td>
</tr>
<tr>
<td>TxProvTxnAbortedRate</td>
<td>The number of provisioning transactions that were aborted due to retry limit per second</td>
</tr>
<tr>
<td>TxProvTxnFailedRate</td>
<td>The number of provisioning transactions that have failed to be started or committed due to errors per second</td>
</tr>
<tr>
<td>TxProvTxnNonDurable</td>
<td>The number of transactions that have been committed, but are not yet durable. Responses for the associated requests are not sent until the transaction has become durable</td>
</tr>
<tr>
<td>TxXsasProvTxnAbortedRate</td>
<td>The number of provisioning SOAP transactions that were aborted due to retry limit per second</td>
</tr>
<tr>
<td>TxXsasProvTxnFailedRate</td>
<td>The number of provisioning SOAP transactions that have failed to be started or committed, due to errors per second</td>
</tr>
<tr>
<td>XsasProvTxnCommittedRate</td>
<td>The number of provisioning SOAP transactions that have been successfully committed per second to the database</td>
</tr>
</tbody>
</table>
Chapter 5
Measurements

Topics:

- General measurements information.....271
- List of measurements.....276

This section provides general information about measurements (including measurement procedures), and lists the measurements that display on measurement reports.
General measurements information

This section provides general information about measurements, measurement-related GUI elements, and measurement report procedures.

Measurements

The measurements framework allows applications to define, update, and produce reports for various measurements.

- Measurements are ordinary counters that count occurrences of different events within the system, for example, the number of messages received. Measurement counters are also called pegs. Additional measurement types provided by the Platform framework are not used in this release.
- Applications simply peg (increment) measurements upon the occurrence of the event that needs to be measured.
- Measurements are collected and merged at the SOAM and NOAM servers as appropriate.
- The GUI allows reports to be generated from measurements.

Measurements that are being pegged locally are collected from shared memory and stored in a disk-backed database table every 5 minutes on all servers in the network. Measurements are collected every 5 minutes on a 5 minute boundary, i.e. at HH:00, HH:05, HH:10, HH:15, and so on. The collection frequency is set to 5 minutes to minimize the loss of measurement data in case of a server failure, and also to minimize the impact of measurements collection on system performance.

All servers in the network (NOAMP, SOAM, and MP servers) store a minimum of 8 hours of local measurements data. More than 5 minutes of local measurements data is retained on each server to minimize loss of measurements data in case of a network connection failure to the server merging measurements.

Measurements data older than the required retention period are deleted by the measurements framework.

Measurements are reported in groups. A measurements report group is a collection of measurement IDs. Each measurement report contains one measurement group. A measurement can be assigned to one or more existing or new measurement groups so that it is included in a measurement report. Assigning a measurement ID to a report group ensures that when you select a report group the same set of measurements is always included in the measurements report.

Note: Measurements from a server may be missing in a report if the server is down; the server is in overload; something in the Platform merging framework is not working; or the report is generated before data is available from the last collection period (there is a 25 to 30 second lag time in availability).

Measurement IDs

Measurement IDs are categorized using a 2-character prefix in the Measurement tag. Possible prefixes include:

- Rx: The measurement is associated with the processing of an incoming message event. This can be the actual count of a particular message received or an event associated with processing of an incoming message.
• **Tx**: The measurement is associated with the processing of an outgoing message event. This can be the actual count of a particular message sent or an event associated with the outgoing message.
• **Tm**: The measurement is associated with the total duration of a particular condition or state during the measurement interval or the min/max/average duration of individual occurrences of a particular condition or state. All Tm measurement values are reported in microseconds.
• **Ev**: The measurement is associated with an event which is not predominantly associated with incoming or outgoing message processing.

**Measurement elements**

This table describes the elements on the Measurements Report page.

**Table 23: Measurements Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Network Elements, Server Groups, Resource Domains, Places and Place Associations for which the measurements report can be run.</td>
<td>Format: Pulldown list&lt;br&gt;Range: Network Elements in the topology; Server Groups in the topology; Resource Domains in the topology; Places in the topology; Place Associations in the topology&lt;br&gt;Note: If no selection is made, the default scope is Entire Network. Default: Entire Network</td>
</tr>
<tr>
<td>Report</td>
<td>A selection of reports</td>
<td>Format: Pulldown list&lt;br&gt;Range: Varies depending on application&lt;br&gt;Default: Group</td>
</tr>
<tr>
<td>Column Filter</td>
<td>The characteristics for filtering the column display</td>
<td>Format: Pulldown list&lt;br&gt;Range: Sub-measurement&lt;br&gt;Sub-measurement Ranges:&lt;br&gt;• Like: A pattern-matching distinction for sub-measurement name, for example, 123* matches any sub-measurement that begins with 123.&lt;br&gt;• In: A list-matching distinction for sub-measurement ID, for example, 3,4,6-10 matches only sub-measurements 3, 4, and 6 through 10.</td>
</tr>
</tbody>
</table>
## Generating a measurements report

Use this procedure to generate and view a measurements report.

1. Select **Measurements > Report**.
   
   The Measurements Report page appears.

2. Select the **Scope**.
   
   For details about this field, or any field on the Measurements Report page, see *Measurement elements*.

3. Select the **Report**.

4. Select the **Interval**.

5. Select the **Time Range**.

6. Select **Beginning** or **Ending** as the **Time Range** interval reference point.

7. Select the **Beginning** or **Ending** date.

8. Click **Go**.

   The report is generated.

   **Note:** Data for the selected scope is displayed in the primary report page. Data for any available sub-scopes are displayed in tabs. For example, if the selected scope is Entire Network, report data for the entire network appears in the primary report page. The individual network entities within the entire network are considered sub-scopes.

9. To view report data for a specific sub-scope, click on the tab for that sub-scope.

   The report data appears.

### Measurements data export elements

This table describes the elements on the Measurements Report Export page.

**Table 24: Schedule Measurement Data Export Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>Name of the scheduled task</td>
<td>Format: Textbox</td>
</tr>
</tbody>
</table>
### Exporting measurements reports

You can schedule periodic exports of data from the **Measurements Report** page. Measurements data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied on the **Measurements Report** 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 transferred to an alternate location using the Export Server feature. For more information about using **Export Server**, see [Data Export](#).

Use this procedure to save a measurements report to the file management storage area. Use this procedure to schedule a data export task.

### Data Input Notes

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Data Input Notes</th>
</tr>
</thead>
</table>
| **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. |
| **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 |
1. Select **Measurements > Report**.

   The **Measurements Report** page appears. For a description of each field, see *Measurement elements*.

2. Generate a measurements report.

   For information about how to generate a measurements report, see *Generating a measurements report*.

3. Click to select the scope or sub-scope measurement report that you want to export.

4. Click **Export**.

   The measurement report is exported to a CSV file. Click the link at the top of the page to go directly to the **Status & Manage > Files** page. From the **Status & Manage** page, you can view a list of files available for download, including the measurements report you exported during this procedure. For more information, see *Opening a file*. The **Schedule Measurement Log Data Export** page appears.

5. Check the **Report Groups** boxes corresponding to any additional measurement reports to be exported.

   **Note:** This step is optional, but is available to allow the export of multiple measurement group reports simultaneously.

6. Select the **Export Frequency**.

   **Note:** If the selected **Export Frequency** is Fifteen Minutes or Hourly, specify the Minutes.

7. Enter the **Task Name**.

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

   **Note:** Task Name is not an option if Export Frequency equals Once.

8. Select the **Time of Day**.

   **Note:** Time of Day is only an option if Export Frequency equals Daily or Weekly.

9. Select the **Day of Week**.

   **Note:** Day of Week is only an option if Export Frequency equals Weekly.

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

    The data export task is scheduled. From the **Status & Manage > Tasks** 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
List of measurements

This section of the document provides a list of all measurements available in the system. Measurements are summarized in tables (by type) with additional measurement details (when available) following each table.

OAM.ALARM measurements

Table 25: OAM Alarm measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm.Crit</td>
<td>The number of critical alarms.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Alarm.Major</td>
<td>The number of major alarms.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Alarm.Minor</td>
<td>The number of minor alarms</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Alarm.State</td>
<td>The alarm state.</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

OAM.SYSTEM measurements

Table 26: OAM System measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>System.CPU_UTIL_PCT_AVERAGE</td>
<td>The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy).</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.CPU_UTIL_PCT_PEAK</td>
<td>The peak CPU usage from 0 to 100% (100% indicates that all cores are completely busy).</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.DISK_UTIL_PCT_AVERAGE</td>
<td>The average disk usage for the partition on which the COMCOL database resides.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.DISK_UTIL_PCT_PEAK</td>
<td>The peak disk usage for the partition on which the COMCOL database resides.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.RAM_UTIL_PCT_AVERAGE</td>
<td>The average committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more...</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>
## Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>System.RAM_UtilPct_Peak</td>
<td>The peak committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.ShMem_UtilPct_Average</td>
<td>The average shared memory usage as a percentage of the limit configured by shl.set.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.ShMem_UtilPct_Peak</td>
<td>The peak shared memory usage as a percentage of the limit configured by shl.set.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapIn_Rate_Average</td>
<td>The average number of memory pages swapped in to memory from disk per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapIn_Rate_Peak</td>
<td>The peak number of memory pages swapped in to memory from disk per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapOut_Rate_Average</td>
<td>The average number of memory pages swapped out of memory from disk per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.SwapOut_Rate_Peak</td>
<td>The peak number of memory pages swapped out of memory from disk per second.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.Swap_UtilPct_Average</td>
<td>The average usage of swap space as a percentage of the total configured swap space.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.Swap_UtilPct_Peak</td>
<td>The peak usage of swap space as a percentage of the total configured swap space.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>System.CPU_CoreUtilPct_Average</td>
<td>The average CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>System.CPU_CoreUtilPct_Peak</td>
<td>The peak CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

### ESPR Measurements

**Table 27: ESPR Measurements**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvAeConvertToProvSubFailed</td>
<td>Total number of failed attempts to convert an auto-enrolled subscriber to a provisioned subscriber</td>
<td>5 minutes</td>
</tr>
<tr>
<td>EvAeProvCreateSubFailed</td>
<td>Total number of failed attempts to create an auto-enrolled subscriber via the provisioning interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>EvAeShCreateSubFailed</td>
<td>Total number of failed attempts to create an auto-enrolled subscriber via the Sh interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>EvAeShDeleteSubFailed</td>
<td>Total number of failed attempts to delete an auto-enrolled subscriber via the Sh interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeConvertToProvSubSuccess</td>
<td>Total number of auto-enrolled subscribers converted to provisioned subscribers</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeProvCreateMsgs</td>
<td>Total number of requests received via the provisioning interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeProvCreateSubSuccess</td>
<td>Total number of auto-enrolled subscribers created via the provisioning interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeShCreateSubSuccess</td>
<td>Total number of auto-enrolled subscribers created via the Sh interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeShDeleteSubMsgs</td>
<td>Total number of unsubscribe requests received via the Sh interface that triggered the removal of an auto-enrolled subscriber</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeShDeleteSubSuccess</td>
<td>Total number of auto-enrolled subscribers deleted via the Sh Interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeShPurCreateMsgs</td>
<td>Total number of update requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxAeShSnrCreateMsgs</td>
<td>Total number of subscribe requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxAeSnrCreateSubSuccess</td>
<td>Total number of auto-enrolled subscribers successfully created via the Sh interface</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrBePnNonPooledEntity</td>
<td>Total number of update requests that generated notification(s) for non-pooled entity(s)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrBePnPooledEntity</td>
<td>Total number of update requests that generated notifications(s) for pooled entity(s)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrBeReadMsgs</td>
<td>Total number of read requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrBeUpdateMsgs</td>
<td>Total number of update requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrNmNotifAck</td>
<td>Total number of notification delivery responses received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrNmNotifAckAsAvailable</td>
<td>Total number of notifications successfully sent to the AS (the AS received the notification)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrNmNotifAckAsUnavailable</td>
<td>Total number of notifications that failed to be sent to the AS (the AS did not receive the notification)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrNmNotifAckLateResponse</td>
<td>Total number of notification delivery responses received after the delivery timeout period expired</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrNmNotifAckNotSubscribed</td>
<td>Total number of notification delivery responses received that indicated the AS was not subscribed to the subscriber</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrNmNotifAckTimeout</td>
<td>Total number of notification delivery requests sent where a response was not received within the configured timeout interval</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrSmSubscribeMsgs</td>
<td>Total number of subscribe requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrSmSubscribeSnoFull</td>
<td>Total number of times when adding a new subscription that the subscription (SNO) record for the subscriber exceeded the maximum number of allowed subscriptions and caused a subscription(s) to be removed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxUdrSmUnsubscribeMsgs</td>
<td>Total number of unsubscribe requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxUdrSmUnsubscribeNsNotFound</td>
<td>Total number of unsubscribe requests where the subscriber exists but the desired notification subscription does not exist</td>
<td>5 minutes</td>
</tr>
<tr>
<td>SQRQuotaRowElementsReset</td>
<td>Total number of Quota Row Elements got reset or the value of the nextResetTime element has been updated. (Pools+Subscribers)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>SQRRecordsExamined</td>
<td>Total number of Records scanned by the Quota Reset Tasks (Pools+Subscribers)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>SQRRecordsFailed</td>
<td>Total number of Records on which Quota Resets or nextResetTime update has Failed (Pools+Subscribers)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>SQRRecordsReset</td>
<td>Total number of Records in which Quota Entities have been reset or the value of the nextResetTime Row Field Element has been updated. (Pools+Subscribers)</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestSuccessfulAll</td>
<td>Total Number of Requests successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeReadReqFailed</td>
<td>Total number of failed read requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeReadReqSuccess</td>
<td>Total number of successful read requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeReadUnkSubscriber</td>
<td>Total number of read requests received where the subscriber was unknown</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateInvalidEntity</td>
<td>Total number of update requests received where an unknown entity was encountered</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateNotPoolMember</td>
<td>Total number of update requests received where a pooled entity was being updated, but the subscriber was not a member of a pool</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateOutOfSync</td>
<td>Total number of update requests received where the incorrect sequence number to perform was supplied</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateReqFailed</td>
<td>Total number of failed update requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateReqSuccess</td>
<td>Total number of successful update requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateTooBusy</td>
<td>Total number of update requests which could not be processed because of congestion</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrBeUpdateUnkSubscriber</td>
<td>Total number of update requests received where the subscriber was unknown</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrNmNotifComAgentError</td>
<td>Total number of notification delivery requests sent that resulted in a ComAgent</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>delivery failure of the notification delivery request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TxUdrNmNotifDeletedTableFull</td>
<td>Total number of notifications that were deleted because the maximum configured number of outstanding notifications allowed had been exceeded</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrNmNotifExceededMaxDel</td>
<td>Total number of notifications that exceeded the maximum configured number of delivery attempts allowed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrNmNotifExceededMaxTtl</td>
<td>Total number of notifications that exceeded the maximum configured time to live</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrNmNotifNoValidEntity</td>
<td>Total number of notifications to be sent that did not consist of any valid entities</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrNmNotifSent</td>
<td>Total number of notification delivery requests sent</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrSmSubscribeReqFailed</td>
<td>Total number of failed subscribe requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrSmSubscribeReqSuccess</td>
<td>Total number of successful subscribe requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrSmSubscribeUnkSubscriber</td>
<td>Total number of subscribe requests received where the subscriber was unknown and was not added via auto-enrollment</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrSmUnsubscribeReqFailed</td>
<td>Total number of failed unsubscribe requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrSmUnsubscribeReqSuccess</td>
<td>Total number of successful unsubscribe requests</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxUdrSmUnsubscribeUnkSubscriber</td>
<td>Total number of unsubscribe requests received where the subscriber was unknown</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

**EvAeConvertToProvSubFailed**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of failed attempts to convert an auto-enrolled subscriber to a provisioned subscriber  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an auto-enrolled subscriber cannot be converted to a provisioned subscriber due to a failure.  
**Measurement Scope:** All  
**Recovery:**
No action required.

**EvAeProvCreateSubFailed**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of failed attempts to create an auto-enrolled subscriber via the provisioning interface  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time there is a failed attempt to create an Auto-Enrolled or Provisioned subscriber.  
**Measurement Scope:** All  
**Recovery:**  
   No action required.

**EvAeShCreateSubFailed**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of failed attempts to create an auto-enrolled subscriber via the provisioning interface  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an attempt to create an auto-enrolled subscriber via an Sh interface request fails.  
**Measurement Scope:** All  
**Recovery:**  
   No action required.

**EvAeShDeleteSubFailed**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of failed attempts to delete an auto-enrolled subscriber via the Sh interface  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an auto-enrolled subscriber cannot be deleted via the Sh interface due to a failure.  
**Measurement Scope:** All  
**Recovery:**  
   No action required.
**RxAeConvertToProvSubSuccess**

**Measurement Group:** Auto Enrollment

**Measurement Type:** Simple

**Description:** Total number of auto-enrolled subscribers converted to provisioned subscribers

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an auto-enrolled subscriber is converted to a provisioned subscriber. This conversion is done when the provisioning system adds or updates profile entity data or when the subscriber is added to a pool.

**Measurement Scope:** All

**Recovery:**

No action required.

---

**RxAeProvCreateMsgs**

**Measurement Group:** Auto Enrollment

**Measurement Type:** Simple

**Description:** Total number of requests received via the provisioning interface where the subscriber was unknown, and auto-enrollment was triggered to create the subscriber

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the UDR Back End processes a provisioning interface request, the subscriber user identity is not found in the index, the update request matches auto-enrollment requirements, and auto-enrollment for provisioning is enabled.

**Measurement Scope:** All

**Recovery:**

No action required.

---

**RxAeProvCreateSubSuccess**

**Measurement Group:** Auto Enrollment

**Measurement Type:** Simple

**Description:** Total number of auto-enrolled subscribers successfully created via the provisioning interface

**Collection Interval:** 5 min

**Peg Condition:** The measurement is incremented each time a subscriber is successfully created via the provisioning interface.

**Measurement Scope:** All

**Recovery:**

No action required.
Rx AeSh Create Sub Success
Measurement Group: Auto Enrollment
Measurement Type: Simple
Description: Total number of auto-enrolled subscribers created via the Sh interface
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an auto-enrolled subscriber is successfully created.
Measurement Scope: All
Recovery: No action required.

Rx AeSh Delete Sub Msgs
Measurement Group: Auto Enrollment
Measurement Type: Simple
Description: Total number of unsubscribe requests received via the Sh interface that triggered the removal of an auto-enrolled subscriber
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an auto-enrolled subscriber is deleted.
Measurement Scope: All
Recovery: No action required.

Rx AeSh Delete Sub Success
Measurement Group: Auto Enrollment
Measurement Type: Simple
Description: Total number of auto-enrolled subscribers successfully deleted via the Sh interface
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a subscriber is successfully deleted via the Sh interface.
Measurement Scope: All
Recovery: No action required.

Rx AeSh Pur Create Msgs
Measurement Group: Auto Enrollment
Measurements

**RxAeShSnrCreateMsgs**

**Measurement Group:** Auto Enrollment  
**Measurement Type:** Simple  
**Description:** Total number of subscribe requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Subscription Manager processes a subscribe request, the subscriber user identity is not found in the index, the subscribe request matches auto-enrollment requirements, and auto-enrollment for SNR is enabled.

**Measurement Scope:** All  
**Recovery:**  
   No action required.

**RxUdrBePnNonPooledEntity**

**Measurement Group:** UDRBE Performance
Measurements

Measurement Type: Simple
Description: Total number of update requests that generated notification(s) for non-pooled entity(s)
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the UDR Back End performs an update of subscriber (non-pool) related data, and one or more subscriptions are found that result in a notification(s) being generated.
Measurement Scope: All
Recovery: No action required.

RxUdrBePnPooledEntity
Measurement Group: UDRBE Performance
Measurement Type: Simple
Description: Total number of update requests that generated notification(s) for pooled entity(s)
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the UDR Back End performs an update of pool related data, and one or more subscriptions are found that result in a notification(s) being generated.
Measurement Scope: All
Recovery: No action required.

RxUdrBeReadMsgs
Measurement Group: UDRBE Performance
Measurement Type: Simple
Description: Total number of read requests received
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the UDR Back End receives a 'read' stack event.
Measurement Scope: All
Recovery: No action required.

RxUdrBeUpdateMsgs
Measurement Group: UDRBE Performance
Measurement Type: Simple
Measurements

**RxUdrNmNotifAck**
- **Measurement Group**: Notification Management
- **Measurement Type**: Simple
- **Description**: Total number of notification delivery responses received
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented each time the Notification Manager receives a 'notifyAck' stack event with a status of other than 'RecipientUnavailable' or 'ResponseTimeout'.
- **Measurement Scope**: All
- **Recovery**: No action required.

**RxUdrNmNotifAckAsAvailable**
- **Measurement Group**: Notification Management
- **Measurement Type**: Simple
- **Description**: Total number of notifications successfully sent to the AS (i.e. the AS received the notification).
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented each time the Notification Manager receives a 'notifyAck' stack event with a status of other than 'RecipientUnavailable' or 'ResponseTimeout'.
- **Measurement Scope**: All
- **Recovery**: No action required.

**RxUdrNmNotifAckAsUnavailable**
- **Measurement Group**: Notification Management
- **Measurement Type**: Simple
- **Description**: Total number of notification delivery responses that indicated that the AS was unavailable
- **Collection Interval**: 5 min
Peg Condition: This measurement is incremented each time the Notification Manager receives a 'notifyAck' stack event with the status 'RecipientUnavailable'.

Measurement Scope: All
Recovery:
   No action required.

RxUdrNmNotifAckLateResponse
Measurement Group: UDRBE Exceptions
Measurement Type: Simple
Description: Total number of notification delivery responses received after the delivery timeout period expired
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Notification Manager receives a 'notifyAck' stack event relating to a notification for which a delivery attempt has been made at least once, the last delivery attempt has already been detected as timed out, and the notification is awaiting a delivery retry.
Measurement Scope: All
Recovery:
   No action required.

RxUdrNmNotifAckNotSubscribed
Measurement Group: Notification Management
Measurement Type: Simple
Description: Total number of notification delivery responses received that indicate the AS was not subscribed to the subscriber
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Notification Manager receives a 'notifyAck' stack event with the status 'NoSubscriptionToData'.
Measurement Scope: All
Recovery:
   No action required.

RxUdrNmNotifAckTimeout
Measurement Group: Notification Management
Measurement Type: Simple
Description: Total number of notification delivery requests sent where a response was not received within the configured timeout interval
Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the Notification Manager sends a ‘notify’ stack event, does not receive a response, and times out.

Measurement Scope: All

Recovery: 
No action required.

RxUdrSmSubscribeMsgs

Measurement Group: Subscription Management

Measurement Type: Simple

Description: Total number of subscribe requests received

Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the Subscription Manager receives a ‘subscribe’ stack event that does not request that the data subscribed to be read and returned in the response.

Measurement Scope: All

Recovery: 
No action required.

RxUdrSmSubscribeSnoFull

Measurement Group: UDRBE Exceptions

Measurement Type: Simple

Description: Total number of times that when adding a new subscription, the SNO record for the subscriber exceeded the maximum number of allowed subscriptions and caused a subscription(s) to be removed

Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the Subscription Manager attempts to add a new (non duplicate) subscription into the SNO record for a subscriber and finds that the SNO record already contains at least the maximum number of subscriptions allowed, per the Maximum Subscriptions per Subscriber configuration option.

Measurement Scope: All

Recovery: 
No action required.

RxUdrSmUnSubscribeMsgs

Measurement Group: Subscription Management

Measurement Type: Simple
Measurements

**Description:** Total number of unsubscribe requests received

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Subscription Manager receives an ‘unsubscribe’ stack event that does not request that the data subscribed to be read and returned in the response.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxUdrSmUnsubscribeNsNotFound**

**Measurement Group:** Subscription Management

**Measurement Type:** Simple

**Description:** Total number of unsubscribe requests where the subscriber exists but the desired notification subscription does not exist

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Subscription Manager processes an unsubscribe request, the subscriber user identity is found in the index, and the notification subscription (NS) to which the unsubscribe request was made is not found in the SNO record for the subscriber.

**Measurement Scope:** All

**Recovery:**

No action required.

**SQRQuotaRowElementsReset**

**Measurement Group:** UDRBE Performance

**Measurement Type:** Simple

**Description:** Total number of quota row elements reset by the quota reset tasks (pools and subscribers).

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented when Quota Reset Scheduler resets each Quota Row Elements in a Subscriber or Pool Record. It is incremented every time a Quota Row Elements is reset in a Subscriber or Pool Record.

**Measurement Scope:** All

**Recovery:**

No action required.

**SQRRecordsExamined**

**Measurement Group:** UDRBE Performance

**Measurement Type:** Simple
**Description:** Total number of records scanned by the quota reset tasks (Pools+Subscribers)

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time quota reset scheduler examines a subscriber or pool record.

**Measurement Scope:** All

**Recovery:**

No action required.

**SQRRecordsFailed**

**Measurement Group:** UDRBE Performance

**Measurement Type:** Simple

**Description:** Total number of Database Records on which Quota Reset Operations have Failed (Pools+Subscribers)

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented when a Quota Reset execution fails in a Subscriber or Pool Record. It is incremented only once irrespective of the number of Quota Row Elements failed in the Subscriber or Pool Record.

**Measurement Scope:** All

**Recovery:**

No action required.

**SQRRecordsReset**

**Measurement Group:** UDRBE Performance

**Measurement Type:** Simple

**Description:** Total number of Records in which at least one Quota Row Elements have been reset (Pools+Subscribers)

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented when Quota Reset Scheduler resets one or more Quota Row Elements in a Subscriber or Pool Record. It is incremented only once, irrespective of the number of Quota Row Elements reset in a Subscriber or Pool Record.

**Measurement Scope:** All

**Recovery:**

No action required.

**TxRequestSuccessfulAll**

**Measurement Group:** UDRFE Performance

**Measurement Type:** Simple
Measurements

**Description:** Total Number of Requests successfully processed
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time an Sh request is successfully processed.
**Measurement Scope:** All
**Recovery:**
   No action required.

**TxUdrBeReadReqFailed**
**Measurement Group:** UDRBE Performance
**Measurement Type:** Simple
**Description:** Total number of failed read requests
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time the UDR Back End processes a read request, and sends a status other than 'Success' in the 'readAck' stack event in response.
**Measurement Scope:** All
**Recovery:**
   No action required.

**TxUdrBeReadReqSuccess**
**Measurement Group:** UDRBE Performance
**Measurement Type:** Simple
**Description:** Total number of successful read requests
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time the UDR Back End processes a read request, and sends a 'Success' status in the 'readAck' stack event in response.
**Measurement Scope:** All
**Recovery:**
   No action required.

**TxUdrBeReadUnkSubscriber**
**Measurement Group:** UDRBE Performance
**Measurement Type:** Simple
**Description:** Total number of read requests received where the subscriber was unknown
**Collection Interval:** 5 min
Peg Condition: This measurement is incremented each time the UDR Back End processes a read request, and the subscriber user identity is not found in the index.

Measurement Scope: All

Recovery:

No action required.

**TxUdrBeUpdateInvalidEntity**

Measurement Group: UDRBE Performance

Measurement Type: Simple

Description: Total number of update requests received where an unknown entity was encountered

Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the UDR Back End processes an update request, and an entity being updated is not found in the SEC.

Measurement Scope: All

Recovery:

No action required.

**TxUdrBeUpdateNotPoolMember**

Measurement Group: UDRBE Performance

Measurement Type: Simple

Description: Total number of update requests received where a pooled entity was being updated, but the subscriber was not a member of a pool

Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the UDR Back End processes an update request for a pooled entity, and the subscriber is not currently a member of a pool.

Measurement Scope: All

Recovery:

No action required.

**TxUdrBeUpdateOutOfSync**

Measurement Group: UDRBE Performance

Measurement Type: Simple

Description: Total number of update requests received where the incorrect sequence number to perform was supplied

Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the UDR Back End processes an update request and the sequence number supplied for one of the entities is not valid.
**Measurement Scope:** All

**Recovery:**

No action required.

**TxUdrBeUpdateReqFailed**

**Measurement Group:** UDRBE Performance  
**Measurement Type:** Simple  
**Description:** Total number of failed update requests  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the UDR Back End processes an update request, and sends a status other than ‘Success’ in the ‘updateAck’ stack event in response.

**Measurement Scope:** All  
**Recovery:**

No action required.

**TxUdrBeUpdateReqSuccess**

**Measurement Group:** UDRBE Performance  
**Measurement Type:** Simple  
**Description:** Total number of successful update requests  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the UDR Back End processes an update request, and sends a ‘Success’ status in the ‘updateAck’ stack event in response.

**Measurement Scope:** All  
**Recovery:**

No action required.

**TxUdrBeUpdateTooBusy**

**Measurement Group:** UDRBE Performance  
**Measurement Type:** Simple  
**Description:** Total number of update requests which could not be processed because of congestion  
**Collection Interval:** 5 min  
**Peg Condition:** The measurement shall be incremented each time the UDR Back End processes fails to process an update request because of congestion, and sends a status other than Success in the updateAck stack event in response.

**Measurement Scope:** All  
**Recovery:**
No action required.

**TxUdrBeUpdateUnkSubscriber**

**Measurement Group:** UDRBE Performance  
**Measurement Type:** Simple  
**Description:** Total number of update requests received where the subscriber was unknown  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the UDR Back End processes an update request, and the subscriber user identity is not found in the index.  
**Measurement Scope:** All  
**Recovery:**  
  No action required.

**TxUdrNmNotifComAgentError**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of notification delivery requests sent that resulted in a ComAgent delivery failure of the notification delivery request  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Notification Manager attempts to send a ‘notify’ stack event and encounters a ComAgent error, resulting in the ‘notify’ stack event not being successfully sent.  
**Measurement Scope:** All  
**Recovery:**  
  No action required.

**TxUdrNmNotifDeletedTableFull**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of notifications that were deleted because the maximum configured number of outstanding notifications allowed was exceeded  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Notification Manager deletes an outstanding notification due to the maximum configured number of outstanding notifications being exceeded.  
**Measurement Scope:** All  
**Recovery:**
No action required.

**TxUdrNmNotifExceededMaxDel**

**Measurement Group:** Notification Management  
**Measurement Type:** Simple  
**Description:** Total number of notifications that exceeded the maximum configured number of delivery attempts allowed  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Notification Manager processes a notification (i.e. a PN) to be sent, checks the number of delivery attempts that have already been made for the notification, and discovers that another delivery attempt would exceed the configured Notification Maximum Delivery Attempts value.  
**Measurement Scope:** All  
**Recovery:**  
No action required.

**TxUdrNmNotifExceededMaxTtl**

**Measurement Group:** Notification Management  
**Measurement Type:** Simple  
**Description:** Total number of notifications that exceeded the maximum configured time to live  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Notification Manager processes a notification (i.e. a PN) to be sent, checks the time difference between when the notification was created and the current date/time, and discovers that the difference is greater than the configured Notification Maximum Time To Live value.  
**Measurement Scope:** All  
**Recovery:**  
No action required.

**TxUdrNmNotifNoValidEntity**

**Measurement Group:** UDRBE Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of notifications to be sent that do not consist of any valid entities  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Notification Manager processes a notification (PN), and every entity to be sent in the ‘notify’ stack event is not valid (i.e. does not exist, or does not contain entity alias information for the interface through which the notification is to be sent).
Measurement Scope: All
Recovery:
   No action required.

**TxUdrNmNotifSent**
Measurement Group: Notification Management
Measurement Type: Simple
Description: Total number of notification delivery requests sent
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Notification Manager sends a ‘notify’ stack event.
Measurement Scope: All
Recovery:
   No action required.

**TxUdrSmSubscribeReqFailed**
Measurement Group: Subscription Management
Measurement Type: Simple
Description: Total number of failed subscribe requests
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Subscription Manager processes a subscribe request and sends a status other than ‘Success’ in the ‘subscribeAck’ stack event in response.
Measurement Scope: All
Recovery:
   No action required.

**TxUdrSmSubscribeReqSuccess**
Measurement Group: Subscription Management
Measurement Type: Simple
Description: Total number of successful subscribe requests
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Subscription Manager processes a subscribe request and sends a ‘Success’ status in the ‘subscribeAck’ stack event in response.
Measurement Scope: All
Recovery:
No action required.

**TxUdrSmSubscribeUnkSubscriber**

**Measurement Group:** Subscription Management  
**Measurement Type:** Simple  
**Description:** Total number of subscribe requests received where the subscriber was unknown and was not added via auto-enrollment  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Subscription Manager processes a subscribe request, the subscriber user identity is not found in the index, and the subscribe request does not match auto-enrollment requirements.  
**Measurement Scope:** All  
**Recovery:**  No action required.

**TxUdrSmUnSubscribeReqFailed**

**Measurement Group:** Subscription Management  
**Measurement Type:** Simple  
**Description:** Total number of failed unsubscribe requests  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Subscription Manager processes an unsubscribe request and sends a status other than 'Success' in the ‘unsubscribeAck’ stack event in response.  
**Measurement Scope:** All  
**Recovery:**  No action required.

**TxUdrSmUnSubscribeReqSuccess**

**Measurement Group:** Subscription Management  
**Measurement Type:** Simple  
**Description:** Total number of successful unsubscribe requests  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Subscription Manager processes an unsubscribe request and sends a ‘Success’ status in the ‘unsubscribeAck’ stack event in response.  
**Measurement Scope:** All  
**Recovery:**  No action required.
TxDrdSmUnSubscribeUnkSubscriber

**Measurement Group:** Subscription Management

**Measurement Type:** Simple

**Description:** Total number of unsubscribe requests received where the subscriber was unknown

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Subscription Manager processes an unsubscribe request, the subscriber user identity is not found in the index.

**Measurement Scope:** All

**Recovery:**

No action required.

**UDRF Measurements**

**Table 28: UDRFE Measurements**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxInvalidDataRefValue</td>
<td>Total number of SNR requests that contained an invalid DataReference AVP value</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxInvalidDelete</td>
<td>Total number of PUR requests that contained a delete request with a sequence number of 0</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxInvalidExpTimeValue</td>
<td>Total number of SNR requests that contained an invalid ExpiryTime AVP value</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestAll</td>
<td>Total number of requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestDiscarded</td>
<td>Total number of requests that were discarded due to the signaling connection being shut down, server being shut down, or transaction not becoming durable within the allowed amount of time</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestFailedAll</td>
<td>Total number of requests that failed to be processed due to errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestFailedPUR</td>
<td>Total number of PUR requests that failed to be processed due to errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestFailedSNR</td>
<td>Total number of SNR requests that failed to be processed due to errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxRequestFailedUDR</td>
<td>Total number of UDR requests that failed to be processed due to errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestPUR</td>
<td>Total number of PUR requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestRejectedComAgentError</td>
<td>Total Number of Requests which cannot be processed due to ComAgent errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestRejectedInvalidServiceInd</td>
<td>Total number of requests that cannot be processed due to invalid service indication</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestRejectedMessageDecodingFailed</td>
<td>Total number of requests that cannot be processed due to message decoding failure</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestRejectedPermissionsNotPresent</td>
<td>Total number of requests that cannot be processed because the host does not have the permissions to execute the operation.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestRejectedUnknownApplicationId</td>
<td>Total number of requests that cannot be processed due to unknown application ID</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestRejectedUnknownUser</td>
<td>Total number of requests that cannot be processed due to unknown user</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestSNR</td>
<td>Total number of SNR requests received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestSuccessfulAll</td>
<td>Total number of requests successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestSuccessfulPUR</td>
<td>Total number of PUR successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestSuccessfulSNR</td>
<td>Total number of SNR successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestSuccessfulUDR</td>
<td>Total number of UDR requests successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxRequestUDR</td>
<td>Total number of UDR received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResetRequestPUR</td>
<td>Total number of PUR Quota Reset Request Messages Received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResetRequestPURFailed</td>
<td>Total number of PUR Quota Reset Requests failed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResetRequestPURSuccessful</td>
<td>Total number of PUR Quota Reset Request Messages successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResponseAll</td>
<td>Total Number of Responses received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResponsePNA</td>
<td>Total number of PNA received</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxResponseRejectedComAgentError</td>
<td>Total number of responses that cannot be processed due to ComAgent connection errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResponseRejectedMessageDecodingFailed</td>
<td>Total number of responses which cannot be processed due to message decoding failure</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxResponseRejectedUnknownApplicationId</td>
<td>Total number of responses which cannot be processed due to unknown application ID</td>
<td>5 minutes</td>
</tr>
<tr>
<td>RxTooMuchData</td>
<td>Total number of PUR requests that contained too much data to process</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmRemotePeerOrphanResponse</td>
<td>Response is received from Remote Diameter Peer for which no pending request event is found</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmPNAReceiveTimeOut</td>
<td>PNR is sent but transaction is timed out as PNA is not received in configured time</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmRemotePeerOrphanResponse</td>
<td>Response is received from Remote Diameter Peer for which no pending request event is found</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmResponseEventTimeOut</td>
<td>Request event is sent to UDRBE but transaction is timed out as UDRBE response event is not received in configured time</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmResponseTimeSPR</td>
<td>Average time from request to response</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrAnsAvgQ</td>
<td>Average UDR answer queue utilization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrAnsPeakQ</td>
<td>Maximum UDR answer queue size utilization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrAvgStkEventQ</td>
<td>Average UDR stack event queue utilization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrbeOrphanResponse</td>
<td>Response event is received from UDRBE for which no pending request event is found</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrPeakStkEventQ</td>
<td>Maximum UDR stack event queue size utilization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrReqAvgQ</td>
<td>Average UDR request queue utilization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TmUdrReqPeakQ</td>
<td>Maximum UDR request queue utilization</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxPnaAsUnavailable</td>
<td>Total number of PNA responses received that indicate an AS is unavailable</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>
### Measurements

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxPnrCreateFailed</td>
<td>Total number of PNR requests that failed to build</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestAll</td>
<td>Total Number of Requests sent</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestFailedAll</td>
<td>Total number of Requests that have failed to be processed due to errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestFailedPNR</td>
<td>Total number of PNR requests that failed to be processed due to errors</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestPNR</td>
<td>Total number of PNR sent to PCRF</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestSuccessfulAll</td>
<td>Total Number of Requests successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxRequestSuccessfulPNR</td>
<td>Total number of PNR requests successfully processed</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxResponseAll</td>
<td>Total number of responses sent</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxResponsePUA</td>
<td>Total number of PUA sent to PCRF</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxResponseSNA</td>
<td>Total number of SNA sent to PCRF</td>
<td>5 minutes</td>
</tr>
<tr>
<td>TxResponseUDA</td>
<td>Total number of UDA sent to PCRF</td>
<td>5 minutes</td>
</tr>
</tbody>
</table>

**RxInvalidDataRefValue**

**Measurement Group:** Sh Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of SNR requests that contained an invalid DataReference AVP value.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an SNR request is received that contains an invalid DataReference AVP value.  
**Measurement Scope:** All  
**Recovery:**  
No action required.

**RxInvalidDelete**

**Measurement Group:** Sh Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of PUR requests that contained a delete request with a sequence number of 0  
**Collection Interval:** 5 min
**Peg Condition**: This measurement is incremented each time a PUR request contains a delete request with a sequence number of 0.

**Measurement Scope**: All

**Recovery**: No action required.

**RxInvalidExpTimeValue**

**Measurement Group**: Sh Exceptions

**Measurement Type**: Simple

**Description**: Total number of SNR requests that contained an invalid ExpireTime AVP value

**Collection Interval**: 5 min

**Peg Condition**: This measurement is incremented each time an SNR request is received that contains an invalid ExpireTime AVP value.

**Measurement Scope**: All

**Recovery**: No action required.

**RxRequestAll**

**Measurement Group**: UDRFE Performance

**Measurement Type**: Simple

**Description**: Total number of requests received

**Collection Interval**: 5 min

**Peg Condition**: This measurement is incremented each time an Sh request is received.

**Measurement Scope**: All

**Recovery**: No action required.

**RxRequestDiscarded**

**Measurement Group**: UDRFE Exception

**Measurement Type**: Simple

**Description**: Total number of requests that have been discarded due to the signaling connection being shut down, server being shut down, or transaction not becoming durable within the allowed amount of time

**Collection Interval**: 5 min

**Peg Condition**: This measurement is incremented each time a request is discarded due to the signaling connection being shut down, server being shut down, or transaction not becoming durable within the allowed amount of time.
Measurements

Measurement Scope: All
Recovery:
    No action required.

RxRequestFailedAll
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Total number of requests that have failed to be processed due to errors
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a request fails to be processed due to errors.
Measurement Scope: All
Recovery:
    No action required.

RxRequestFailedPUR
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Total number of PUR requests that have failed to be processed due to errors
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a PUR request fails to be processed due to errors.
Measurement Scope: All
Recovery:
    No action required.

RxRequestFailedSNR
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Total number of SNR requests that have failed to be processed due to errors
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an SNR request fails to be processed due to errors.
Measurement Scope: All
Recovery:
No action required.

**RxRequestFailedUDR**

**Measurement Group:** UDRFE Performance  
**Measurement Type:** Simple  
**Description:** Total number of UDR requests that have failed to be processed due to errors  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a UDR request fails to be processed due to errors.

**Measurement Scope:** All  
**Recovery:**  
   No action required.

**RxRequestPUR**

**Measurement Group:** Sh Performance  
**Measurement Type:** Simple  
**Description:** Total number of PUR requests received  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a PUR request is received.

**Measurement Scope:** All  
**Recovery:**  
   No action required.

**RxRequestRejectedComAgentError**

**Measurement Group:** Sh Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of requests that cannot be processed due to ComAgent connection errors  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a request cannot be processed due to ComAgent connection errors.

**Measurement Scope:** All  
**Recovery:**  
   No action required.
RxRequestRejectedInvalidServiceInd
 Measurement Group: Sh Performance
 Measurement Type: Simple
 Description: Total number of requests that cannot be processed due to invalid service indication
 Collection Interval: 5 min
 Peg Condition: This measurement is incremented each time a request cannot be processed due to invalid service indication.
 Measurement Scope: All
 Recovery: 
 No action required.

RxRequestRejectedMessageDecodingFailed
 Measurement Group: UDRFE Performance
 Measurement Type: Simple
 Description: Total number of requests that cannot be processed due to message decoding failure
 Collection Interval: 5 min
 Peg Condition: This measurement is incremented each time a request cannot be processed due to message decoding failure.
 Measurement Scope: All
 Recovery: 
 No action required.

RxRequestRejectedPermissionsNotPresent
 Measurement Group: Sh Exceptions
 Measurement Type: Simple
 Description: Total number of requests that cannot be processed because the host does not have the permissions to execute the operation
 Collection Interval: 5 min
 Peg Condition: This measurement is incremented each time a request cannot be processed because the host does not have the permissions to execute the operation.
 Measurement Scope: All
 Recovery: 
 No action required.
Measurments

RxRequestRejectedUnknownApplicationId
Measurement Group: Sh Exceptions
Measurement Type: Simple
Description: Total number of requests that cannot be processed because of an unknown application ID
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a request cannot be processed because of an unknown application ID.
Measurement Scope: All
Recovery:
   No action required.

RxRequestRejectedUnknownUser
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Total number of requests that cannot be processed because of an unknown user
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a request cannot be processed because of an unknown user.
Measurement Scope: All
Recovery:
   No action required.

RxRequestSNR
Measurement Group: Sh Performance
Measurement Type: Simple
Description: Total number of SNR requests received
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an SNR request is received.
Measurement Scope: All
Recovery:
   No action required.

RxRequestSuccessfulAll
Measurement Group: UDRFE Performance
**Measurement Type:** Simple  
**Description:** Total number of requests successfully processed  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a request is successfully processed.  
**Measurment Scope:** All  
**Recovery:**  
  No action required.

**RxRequestSuccessfulPUR**  
**Measurement Group:** UDRFE Performance  
**Measurement Type:** Simple  
**Description:** Total number of PUR requests successfully processed  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a PUR request is successfully processed.  
**Measurement Scope:** All  
**Recovery:**  
  No action required.

**RxRequestSuccessfulSNR**  
**Measurement Group:** UDRFE Performance  
**Measurement Type:** Simple  
**Description:** Total number of SNR requests successfully processed  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an SNR request is successfully processed.  
**Measurement Scope:** All  
**Recovery:**  
  No action required.

**RxRequestSuccessfulUDR**  
**Measurement Group:** UDRFE Performance  
**Measurement Type:** Simple  
**Description:** Total number of UDR requests successfully processed  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a UDR request is successfully processed.
Measurements

**RxRequestUDR**
- **Measurement Group**: Sh Performance
- **Measurement Type**: Simple
- **Description**: Total number of UDR requests received
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented each time a UDR request is received.

**RxResetRequestPUR**
- **Measurement Group**: UDRBE Performance
- **Measurement Type**: Simple
- **Description**: Total number of PUR Quota Reset Request Messages Received
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented when a PUR Reset message arrives at Sh Interface.

**RxResetRequestPURFailed**
- **Measurement Group**: UDRBE Performance
- **Measurement Type**: Simple
- **Description**: Total number of PUR quota reset requests failed
- **Collection Interval**: 5 min
- **Peg Condition**: This measurement is incremented when a PUR reset request fails.
**RxResetRequestPURSuccessful**

**Measurement Group:** UDRBE Performance  
**Measurement Type:** Simple  
**Description:** Total number of PUR quota reset request messages successfully processed  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented when a PUR reset request completes successfully and a response is sent.  
**Measurement Scope:** All  
**Recovery:**  
No action required.

**RxResponseAll**

**Measurement Group:** UDRFE Performance  
**Measurement Type:** Simple  
**Description:** Total Number of Responses received  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an Sh response is received.  
**Measurement Scope:** All  
**Recovery:**  
No action required.

**RxResponsePNA**

**Measurement Group:** Sh Performance  
**Measurement Type:** Simple  
**Description:** Total number of PNA responses received  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a PNA response is received.  
**Measurement Scope:** All  
**Recovery:**  
No action required.

**RxResponseRejectedComAgentError**

**Measurement Group:** Sh Exceptions  
**Measurement Type:** Simple
Measurements

**Description:** Total number of responses that cannot be processed due to ComAgent connection errors

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a response cannot be processed due to ComAgent connection errors.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxResponseRejectedMessageDecodingFailed**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** Total number of responses that cannot be processed due to message decoding failure

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a response cannot be processed due to message decoding failure.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxResponseRejectedUnknownApplicationId**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** Total number of responses that cannot be processed due to an unknown application ID

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a response cannot be processed due to an unknown application ID.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxTooMuchData**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** Total number of PUR requests that contain too much data to process

**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time a PUR request contains too much data to process.

**Measurement Scope:** All

**Recovery:**

No action required.

**TmRemotePeerOrphanResponse**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** Response event is received from Remote Diameter Peer for which no pending request event is found.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a response event is received from Remote Diameter Peer for which no pending request event is found.

**Measurement Scope:** All

**Recovery:**

No action required.

**TmPNAReceiveTimeOut**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** A PNR is sent but the transaction is timed out because a PNA is not received in configured time.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a PNR is sent but the transaction is timed out because a PNA is not received in configured time.

**Measurement Scope:** All

**Recovery:**

No action required.
Measurements

**Peg Condition:** This measurement is incremented each time a response event is received from Remote Diameter Peer for which no pending request event is found.

**Measurement Scope:** All

**Recovery:**

No action required.

**TmResponseEventTimeOut**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** A request event is sent to UDRBE but the transaction is timed out because a UDRBE response event is not received in configured time

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a request event is sent to UDRBE but the transaction is timed out because a UDRBE response event is not received in configured time.

**Measurement Scope:** All

**Recovery:**

No action required.

**TmResponseTimeSPR**

**Measurement Group:** UDRFE Performance

**Measurement Type:** Average

**Description:** Average time from request to response

**Collection Interval:** 5 min

**Peg Condition:** This measurement maintains the average time from request to response for Sh messages received.

**Measurement Scope:** All

**Recovery:**

No action required.

**TmUdrAnsAvgQ**

**Measurement Group:** UDRFE Performance

**Measurement Type:** Single

**Description:** Average UDR answer task event queue utilization

**Collection Interval:** 5 min

**Peg Condition:** This measurement maintains the average UDR answer task event queue size utilization.

**Measurement Scope:** All
Recovery:
   No action required.

**TmUdrAnsPeakQ**
*Measurement Group:* UDRFE Exceptions
*Measurement Type:* Single
*Description:* Maximum UDR Answer queue utilization
*Collection Interval:* 5 min
*Peg Condition:* This measurement maintains the maximum UDR answer task event queue size utilization.
*Measurement Scope:* All
*Recovery:* No action required.

**TmUdrAvgStkEventQ**
*Measurement Group:* UDRFE Performance
*Measurement Type:* Average
*Description:* Average UDR stack event queue utilization
*Collection Interval:* 5 min
*Peg Condition:* This measurement maintains the average UDR stack event queue utilization.
*Measurement Scope:* All
*Recovery:* No action required.

**TmUdrbeOrphanResponse**
*Measurement Group:* Sh Exceptions
*Measurement Type:* Simple
*Description:* Response event is received from UDRBE for which no pending request event is found
*Collection Interval:* 5 min
*Peg Condition:* This measurement is incremented each time a response event is received from UDRBE for which no pending request event is found.
*Measurement Scope:* All
*Recovery:* No action required.
**TmUdrPeakStkEventQ**
Measurement Group: UDRFE Performance
Measurement Type: Maximum
Description: Maximum UDR stack event queue size utilization
Collection Interval: 5 min
Peg Condition: This measurement maintains the maximum UDR stack event queue size utilization.
Measurement Scope: All
Recovery: No action required.

**TmUdrReqAvgQ**
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Average UDR request task event queue utilization
Collection Interval: 5 min
Peg Condition: This measurement maintains the average UDR request task event queue size utilization.
Measurement Scope: All
Recovery: No action required.

**TmUdrReqPeakQ**
Measurement Group: UDRFE Exceptions
Measurement Type: Simple
Description: Maximum UDR request task event queue utilization
Collection Interval: 5 min
Peg Condition: This measurement maintains the maximum UDR request task event queue size utilization.
Measurement Scope: All
Recovery: No action required.

**TxPnaAsUnavailable**
Measurement Group: Sh Exceptions
Measurement Type: Simple
Measurements

**Description:** Total number of PNA responses received that indicate an AS is unavailable

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a received PNA response indicates that an AS is unavailable.

**Measurement Scope:** All

**Recovery:**

No action required.

**TxPnrCreateFailed**

**Measurement Group:** Sh Exceptions

**Measurement Type:** Simple

**Description:** Total number of PNR requests that failed to build

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a PNR request fails to be built.

**Measurement Scope:** All

**Recovery:**

No action required.

**TxRequestAll**

**Measurement Group:** UDRFE Performance

**Measurement Type:** Simple

**Description:** Total number of Requests sent

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an Sh request is sent.

**Measurement Scope:** All

**Recovery:**

No action required.

**TxRequestFailedAll**

**Measurement Group:** UDRFE Performance

**Measurement Type:** Simple

**Description:** Total number of Requests that have failed to be processed due to errors

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a request has failed to be processed due to errors.
Measurements

TxRequestPNR
Measurement Group: Sh Performance
Measurement Type: Simple
Description: Total number of PNR requests sent to the PCRF
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a PNR request is sent.
Recovery: All

No action required.

TxRequestFailedPNR
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Total number of PNR requests that failed to be processed due to errors
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a PNR request fails to be processed due to errors.
Recovery: All

No action required.

TxRequestSuccessfulAll
Measurement Group: UDRFE Performance
Measurement Type: Simple
Description: Total number of requests successfully processed
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an Sh request is successfully processed.
Recovery: All

No action required.
**TxRequestSuccessfulPNR**
- **Measurement Group:** UDRFE Performance
- **Measurement Type:** Simple
- **Description:** Total number of PNR requests successfully processed
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented each time a PNR request is successfully processed.
- **Measurement Scope:** All
- **Recovery:**
  - No action required.

**TxResponseAll**
- **Measurement Group:** UDRFE Performance
- **Measurement Type:** Simple
- **Description:** Total number of responses sent
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented each time an Sh response is sent.
- **Measurement Scope:** All
- **Recovery:**
  - No action required.

**TxResponsePUA**
- **Measurement Group:** Sh Performance
- **Measurement Type:** Simple
- **Description:** Total number of PUA responses sent to the PCRF
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented each time a PUA response is sent.
- **Measurement Scope:** All
- **Recovery:**
  - No action required.

**TxResponseSNA**
- **Measurement Group:** Sh Performance
- **Measurement Type:** Simple
- **Description:** Total number of SNA responses sent to the PCRF
Collection Interval: 5 min

Peg Condition: This measurement is incremented each time an SNA response is sent.

Measurement Scope: All

Recovery: No action required.

**TxResponseUDA**

Measurement Group: Sh Performance

Measurement Type: Simple

Description: Total number of UDA responses sent to the PCRF

Collection Interval: 5 min

Peg Condition: This measurement is incremented each time a UDA response is sent.

Measurement Scope: All

Recovery: No action required.

### UDR RAS and XSAS Provisioning Interface Measurements

The provisioning interface measurement group is a set of measurements associated with the usage of provisioning rules. These measurements will allow the user to determine which provisioning rules are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed.

**Table 29: UDR RAS and XSAS Provisioning Related Measurements**

<table>
<thead>
<tr>
<th>Measurement Tag</th>
<th>Description</th>
<th>Collection Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProvTxnCommitted</td>
<td>Total number of transactions successfully committed to the database (memory and on disk) on the active server of the primary site</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvExportCmds</td>
<td>Total number of commands exported</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvExportRequested</td>
<td>Total number of exports requested</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvExportsFailed</td>
<td>Total number of XML export requests that failed due to errors</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvExportsSuccessful</td>
<td>Total number of successful XML export requests</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvImportCmdsFailed</td>
<td>Total number of commands that failed import</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxProvImportCmdsSuccessful</td>
<td>Total number of commands that imported successfully</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvImportFilesFailed</td>
<td>Total number of files that failed to be imported due to errors</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvImportFilesReceived</td>
<td>Total number of provisioning files received from an import operation</td>
<td>5 min</td>
</tr>
<tr>
<td>RxProvImportFilesSuccessful</td>
<td>Total number of files imported successfully</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasDeleteReqReceived</td>
<td>Total number of REST DELETE requests that have been received on the provision interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasGetReqReceived</td>
<td>Total number of REST GET requests that have been received on the provision interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasPostReqReceived</td>
<td>Total number of REST POST requests that have been received on the provision interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvConnectionIdleTimeouts</td>
<td>Total number of connections that timed out and terminated due to idleness</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvConnectsAccepted</td>
<td>Total number of client initiated connect attempts that were accepted</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvConnectsAttempted</td>
<td>Total number of client initiated connect attempts to establish a connection with the server</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvConnectsDenied</td>
<td>Total number of client initiated connect attempts denied because clients were not running on an authorized server, or the maximum number of allowed connections was already established</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvMsgsDiscarded</td>
<td>Total number of provisioning messages discarded because the connection was shut down, the server was shut down, the server role switched from active to standby, or the transaction did not become durable within the allowed amount of time</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvMsgsFailed</td>
<td>Total number of provisioning messages that failed to be processed due to errors</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvMsgsReceived</td>
<td>Total number of provisioning messages received</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasProvMsgsSent</td>
<td>Total number of provisioning messages sent</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxRasProvMsgsSuccessful</td>
<td>Total number of provisioning messages successfully processed</td>
<td>5 min</td>
</tr>
<tr>
<td>RxRasPutReqReceived</td>
<td>Total number of REST PUT requests that have been received on the provisioning interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasDeleteReqReceived</td>
<td>Total number of SOAP delete requests that have been received on the provisioning interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasInsertReqReceived</td>
<td>The total number of SOAP insert requests that have been received on the provisioning interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasOperationReqReceived</td>
<td>Total number of SOAP operation requests that have been received on the provisioning interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvConnectionIdleTimeouts</td>
<td>Total number of connections that timed out and terminated due to idleness</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvConnectsAccepted</td>
<td>Total number of client initiated connect attempts that were accepted</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvConnectsAttempted</td>
<td>Total number of client initiated connect attempts to establish a connection with the server</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvConnectsDenied</td>
<td>Total number of client initiated connect attempts denied because the clients were not running on an authorized server, or the maximum number of allowed connections was already established</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvConnectsFailed</td>
<td>Total number of client initiated connect attempts that failed due to errors during initialization</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvMsgsDiscarded</td>
<td>Total number of provisioning messages discarded because the connection was shut down, the server was shutdown, the server role switched from active to standby, or the transaction did not become durable within the allowed amount of time</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvMsgsFailed</td>
<td>Total number of provisioning messages that failed to be processed due to errors</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvMsgsReceived</td>
<td>Total number of provisioning messages received</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvMsgsSent</td>
<td>Total number of provisioning messages sent</td>
<td>5 min</td>
</tr>
<tr>
<td>Measurement Tag</td>
<td>Description</td>
<td>Collection Interval</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>RxXsasProvMsgsSuccessful</td>
<td>Total number of provisioning messages that were successfully processed</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvTxnRequestsDiscarded</td>
<td>The total number of SOAP transactions that have been discarded due to the connection being shutdown, server being shutdown, server’s role switching from active to standby, or transaction not becoming durable within the allowed amount of time</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasProvTxnTotal</td>
<td>The total number of SOAP Transactions that have been attempted</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasSelectReqReceived</td>
<td>Total number of SOAP select requests that have been received on the provisioning interface</td>
<td>5 min</td>
</tr>
<tr>
<td>RxXsasUpdateReqReceived</td>
<td>Total number of SOAP update requests that have been received on the provisioning interface</td>
<td>5 min</td>
</tr>
<tr>
<td>TxProvImportResultFilesTransferred</td>
<td>Total number of result files transferred</td>
<td>5 min</td>
</tr>
<tr>
<td>TxProvTxnAborted</td>
<td>Total number of transactions that were successfully aborted after a configured number of retries</td>
<td>5 min</td>
</tr>
<tr>
<td>TxProvTxnDurabilityTimeouts</td>
<td>Total number of committed, non-durable transactions that failed to become durable within the amount of time specified by Transaction Durability Timeout</td>
<td>5 min</td>
</tr>
<tr>
<td>TxProvTxnFailed</td>
<td>Total number of transactions that failed to be started or committed or were aborted due to errors</td>
<td>5 min</td>
</tr>
<tr>
<td>TxProvTxnTotal</td>
<td>Total number of transactions that were attempted (the sum of R_ProvTxnCommitted, R_ProvTxnTimeouts, R_ProvTxnAborted, and R_ProvTxnFailed counters)</td>
<td>5 min</td>
</tr>
<tr>
<td>TxXsasProvTxnAborted</td>
<td>The total number of SOAP transactions that have been aborted after configured number of retries</td>
<td>5 min</td>
</tr>
<tr>
<td>TxXsasProvTxnFailed</td>
<td>The total number of SOAP transactions that have failed to be started or committed</td>
<td>5 min</td>
</tr>
<tr>
<td>XsasProvTxnCommitted</td>
<td>The total number of Soap transactions that have been successfully committed to the database</td>
<td>5 min</td>
</tr>
</tbody>
</table>
**ProvTxnCommitted**

*Measurement Group:* Provisioning Performance  
*Measurement Type:* Simple  
*Description:* Total number of transactions that were successfully committed to the database (memory and on disk) on the active server of the primary site  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement is incremented each time a transaction is successfully committed to the database (memory and on disk) on the active server of the primary site.  
*Measurement Scope:* All  
*Recovery:*  
No action required.

**RxProvExportCmds**

*Measurement Group:* Provisioning Performance  
*Measurement Type:* Simple  
*Description:* Total number of commands exported  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement is incremented each time a command is exported.  
*Measurement Scope:* All  
*Recovery:*  
No action required.

**RxProvExportRequested**

*Measurement Group:* Provisioning Performance  
*Measurement Type:* Simple  
*Description:* Total number of exports requested.  
*Collection Interval:* 5 min  
*Peg Condition:* This measurement is incremented each time an export is requested.  
*Measurement Scope:* All  
*Recovery:*  
No action required.

**RxProvExportsFailed**

*Measurement Group:* Provisioning Exceptions
Measurements

**Measurement Type:** Simple
**Description:** Total number of XML export requests that failed due to errors
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time an XML export request fails due to errors.
**Measurement Scope:** All
**Recovery:**

No action required.

**RxProvExportsSuccessful**
**Measurement Group:** Provisioning Performance
**Measurement Type:** Simple
**Description:** Total number of successful XML export requests
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time there is a successful XML export request.
**Measurement Scope:** All
**Recovery:**

No action required.

**RxProvImportCmdsFailed**
**Measurement Group:** Provisioning Exceptions
**Measurement Type:** Simple
**Description:** Total number of commands that failed import
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time a command import fails.
**Measurement Scope:** All
**Recovery:**

No action required.

**RxProvImportCmdsSuccessful**
**Measurement Group:** Provisioning Performance
**Measurement Type:** Simple
**Description:** Total number of provisioning commands that imported successfully
**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time a provisioning command is imported successfully.
Measurements

Measurement Scope: All
Recovery:
   No action required.

RxProvImportFilesFailed
Measurement Group: Provisioning Exceptions
Measurement Type: Simple
Description: Total number of files that failed to be imported due to errors
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a file import fails due to errors.
Measurement Scope: All
Recovery:
   No action required.

RxProvImportFilesReceived
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: Total number of provisioning files received from an import operation
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a provisioning file is received from an import operation.
Measurement Scope: All
Recovery:
   No action required.

RxProvImportFilesSuccessful
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: Total number of files imported successfully
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a file is imported successfully.
Measurement Scope: All
Recovery:
   No action required.
**RxProvImportResultFilesTransferred**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of import result files transferred  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a import result file is transferred successfully.

**Measurement Scope:** All  
**Recovery:**  
No action required.

**RxRasDeleteReqReceived**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of REST DELETE requests that have been received on the provisioning interface  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Provisioning Front End receives a DELETE request on the REST provisioning interface.

**Measurement Scope:** All  
**Recovery:**  
No action required.

**RxRasGetReqReceived**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of REST GET requests that have been received on the provisioning interface  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time the Provisioning Front End receives a GET request on the REST provisioning interface.

**Measurement Scope:** All  
**Recovery:**  
No action required.
**RxRasPostReqReceived**

**Measurement Group:** Provisioning Performance

**Measurement Type:** Simple

**Description:** Total number of REST POST requests that have been received on the provisioning interface

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time the Provisioning Front End receives a POST request on the REST provisioning interface.

**Measurement Scope:** All

**Recovery:**

No action required.

---

**RxRasProvConnectionIdleTimeouts**

**Measurement Group:** Provisioning Exceptions

**Measurement Type:** Simple

**Description:** Total number of connections that timed out and terminated due to idleness

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an RAS connection times out due to being idle too long.

**Measurement Scope:** All

**Recovery:**

No action required.

---

**RxRasProvConnectsAccepted**

**Measurement Group:** Provisioning Performance

**Measurement Type:** Simple

**Description:** Total number of client initiated connect attempts that were accepted

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an RAS client attempts to initiate a connection with the server.

**Measurement Scope:** All

**Recovery:**

No action required.

---

**RxRasProvConnectsAttempted**

**Measurement Group:** Provisioning Performance
Measurement Type: Simple
Description: Total number of client initiated attempts to establish a connection with the server
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an RAS client attempts to initiate a connection with the server.
Measurement Scope: All
Recovery: No action required.

RxRasProvConnectsDenied
Measurement Group: Provisioning Exceptions
Measurement Type: Simple
Description: Total number of client initiated connect attempts that were denied because clients were not running on an authorized server, or the maximum number of allowed connections was already established
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an RAS client attempts to initiate a connection, and the connection is denied because clients are not running on an authorized server, or the maximum number of allowed connections is already established or the provisioning interface is disabled.
Measurement Scope: All
Recovery: No action required.

RxRasProvMsgsDiscarded
Measurement Group: Provisioning Exceptions
Measurement Type: Simple
Description: Total number of provisioning messages that were discarded because the connection was shut down, the server was shut down, the server role switched from active to standby, or the transaction did not become durable within the allowed amount of time.
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time an RAS provisioning message is discarded because the connection is shut down, the server is shut down, the server role switches from active to standby, or the transaction does not become durable within the allowed amount of time.
Measurement Scope: All
Recovery: No action required.
**RxRasProvMsgsFailed**

**Measurement Group:** Provisioning Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of provisioning messages that failed to be processed due to errors  
**Collection Interval:** 5 min  
** Peg Condition:** This measurement is incremented each time a received RAS provisioning message fails to be processed due to errors.  
** Measurement Scope:** All  
**Recovery:** No action required.

**RxRasProvMsgsReceived**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of provisioning messages that were received  
**Collection Interval:** 5 min  
** Peg Condition:** This measurement is incremented each time an RAS provisioning message is received.  
** Measurement Scope:** All  
**Recovery:** No action required.

**RxRasProvMsgsSent**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of provisioning messages that were sent  
**Collection Interval:** 5 min  
** Peg Condition:** This measurement is incremented each time an RAS provisioning message is sent.  
** Measurement Scope:** PROV Group  
**Recovery:** No action required.

**RxRasProvMsgsSuccessful**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple
Measurements

**Description**: Total number of provisioning messages that were successfully processed

**Collection Interval**: 5 min

**Peg Condition**: This measurement is incremented each time a received RAS provisioning message is successfully processed.

**Measurement Scope**: All

**Recovery**: No action required.

**RxRasPutReqReceived**

**Measurement Group**: Provisioning Performance

**Measurement Type**: Simple

**Description**: Total number of REST PUT requests that have been received on the provisioning interface

**Collection Interval**: 5 min

**Peg Condition**: This measurement is incremented each time the Provisioning Front End receives a PUT request on the REST provisioning interface.

**Measurement Scope**: All

**Recovery**: No action required.

**RxXsasDeleteReqReceived**

**Measurement Group**: Provisioning Performance

**Measurement Type**: Simple

**Description**: Total number of SOAP delete requests that have been received on the provisioning interface

**Collection Interval**: 5 min

**Peg Condition**: This measurement is incremented each time the Provisioning Front End receives a delete request on the SOAP provisioning interface.

**Measurement Scope**: All

**Recovery**: No action required.

**RxXsasInsertReqReceived**

**Measurement Group**: Provisioning Performance

**Measurement Type**: Simple

**Description**: Total number of SOAP insert requests that have been received on the provisioning interface
Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the Provisioning Front End receives an insert request on the SOAP provisioning interface.

Measurement Scope: All

Recovery: No action required.

RxXsasOperationReqReceived
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: Total number of SOAP operation requests that have been received on the provisioning interface
Collection Interval: 5 min

Peg Condition: This measurement is incremented each time the Provisioning Front End receives an operation request on the SOAP provisioning interface.

Measurement Scope: All

Recovery: No action required.

RxXsasProvConnectionIdleTimeouts
Measurement Group: Provisioning Exceptions
Measurement Type: Simple
Description: Total number of connections that timed out and terminated due to idleness
Collection Interval: 5 min

Peg Condition: This measurement is incremented each time an XSAS connection times out due to being idle too long.

Measurement Scope: All

Recovery: No action required.

RxXsasProvConnectsAccepted
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: Total number of client initiated connect attempts that were accepted
Collection Interval: 5 min
**Peg Condition:** This measurement is incremented each time an XSAS client initiates a connection that is accepted.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxXsasProvConnectsAttempted**

**Measurement Group:** Provisioning Performance

**Measurement Type:** Simple

**Description:** Total number of client initiated attempts to establish a connection with the server.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an XSAS client attempts to initiate a connection with the server.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxXsasProvConnectsDenied**

**Measurement Group:** Provisioning Exceptions

**Measurement Type:** Simple

**Description:** Total number of client initiated connect attempts that were denied because clients were not running on an authorized server, the maximum number of allowed connections was already established.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an XSAS client attempts to initiate a connection, and the connection is denied because clients are not running on an authorized server, or the maximum number of allowed connections is already established.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxXsasProvConnectsFailed**

**Measurement Group:** Provisioning Exceptions

**Measurement Type:** Simple

**Description:** Total number of client initiated connect attempts that failed due to errors during initialization.

**Collection Interval:** 5 min
**Peg Condition:** This measurement is incremented each time an XSAS client attempts a connection that failed due to errors during initialization.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxXsasProvMsgsDiscarded**

**Measurement Group:** Provisioning Exceptions

**Measurement Type:** Simple

**Description:** Total number of provisioning messages that were discarded because the connection was shut down, the server was shut down, the server role switched from active to standby, or the transaction did not become durable within the allowed amount of time.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an XSAS provisioning message is discarded because the connection is shut down, the server is shut down, the server role switched from active to standby, or the transaction does not become durable within the allowed amount of time.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxXsasProvMsgsFailed**

**Measurement Group:** Provisioning Exceptions

**Measurement Type:** Simple

**Description:** Total number of provisioning messages that failed to be processed due to errors.

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time a received XSAS provisioning message fails to be processed due to errors.

**Measurement Scope:** All

**Recovery:**

No action required.

**RxXsasProvMsgsReceived**

**Measurement Group:** Provisioning Performance

**Measurement Type:** Simple

**Description:** Total number of provisioning messages that were received

**Collection Interval:** 5 min

**Peg Condition:** This measurement is incremented each time an XSAS provisioning message is received.
**Measurements**

**RxXsasProvMsgsSent**
- **Measurement Group:** Provisioning Performance
- **Measurement Type:** Simple
- **Description:** Total number of provisioning messages that were sent
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented each time an XSAS provisioning message is sent.
- **Recovery:** No action required.

**RxXsasProvMsgsSuccessful**
- **Measurement Group:** Provisioning Performance
- **Measurement Type:** Simple
- **Description:** The total number of provisioning messages that were successfully processed
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement is incremented each time a received XSAS provisioning message is successfully processed.
- **Recovery:** No action required.

**RxXsasProvTxnRequestsDiscarded**
- **Measurement Group:** Provisioning Exceptions
- **Measurement Type:** Simple
- **Description:** The total number of SOAP transactions that have been discarded due to the connection being shutdown, server being shutdown, server’s role switching from active to standby, or transaction not becoming durable within the allowed amount of time.
- **Collection Interval:** 5 min
- **Peg Condition:** This measurement shall be incremented each time a SOAP transaction has been discarded due to the connection being shutdown, server being shutdown, server’s role switching from active to standby, or transaction not becoming durable within the allowed amount of time.
- **Recovery:** No action required.
Recovery:
No action required.

RxXsasProvTxnTotal
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: The total number of SOAP transactions that have been received
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time a SOAP transaction has been received.
Measurement Scope: All
Recovery:
No action required.

RxXsasSelectReqReceived
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: Total number of SOAP select requests that have been received on the provisioning interface
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Provisioning Front End receives a select request on the SOAP provisioning interface.
Measurement Scope: All
Recovery:
No action required.

RxXsasUpdateReqReceived
Measurement Group: Provisioning Performance
Measurement Type: Simple
Description: Total number of SOAP update requests that have been received on the provisioning interface
Collection Interval: 5 min
Peg Condition: This measurement is incremented each time the Provisioning Front End receives an update request on the SOAP provisioning interface.
Measurement Scope: All
Recovery:
No action required.
Measurements

TxProvImportResultFilesTransferred

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of import result files transferred  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time an import result file is transferred.  
**Measurement Scope:** All  
**Recovery:** No action required.

TxProvTxnAborted

**Measurement Group:** Provisioning Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of transactions that were aborted after the configured number of retries.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a transaction is aborted because the configured number of retries were already exhausted.  
**Measurement Scope:** All  
**Recovery:** No action required.

TxProvTxnDurabilityTimeouts

**Measurement Group:** Provisioning Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of committed, non-durable transactions that failed to become durable within the amount of time specified by the Transaction Durability Timeout value  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a committed, non-durable transaction fails to become durable within the amount of time specified by the Transaction Durability Timeout value.  
**Measurement Scope:** All  
**Recovery:** No action required.
**TxProvTxnFailed**

**Measurement Group:** Provisioning Exceptions  
**Measurement Type:** Simple  
**Description:** Total number of transactions that failed to be started or committed.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a transaction fails to be started or committed.  
**Measurement Scope:** All  
**Recovery:**  
   No action required.

**TxProvTxnTotal**

**Measurement Group:** Provisioning Performance  
**Measurement Type:** Simple  
**Description:** Total number of transactions that were attempted  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement is incremented each time a transaction is attempted.  
**Measurement Scope:** All  
**Recovery:**  
   No action required.

**TxXsasProvTxnAborted**

**Measurement Group:** Provisioning Exceptions  
**Measurement Type:** Simple  
**Description:** The total number of SOAP transactions that have been aborted after configured number of retries.  
**Collection Interval:** 5 min  
**Peg Condition:** This measurement shall be incremented each time a SOAP transaction has been aborted after configured number of retries is reached.  
**Measurement Scope:** All  
**Recovery:**  
   No action required.

**TxXsasProvTxnFailed**

**Measurement Group:** Provisioning Exceptions
Measurements

**Measurement**

**Type:** Simple

**Description:** The total number of SOAP transactions that have failed to be started or committed.

**Collection Interval:** 5 min

**Peg Condition:** This measurement shall be incremented each time a SOAP transaction has failed to be started or committed.

**Measurement Scope:** All

**Recovery:**

No action required.

---

**XsasProvTxnCommitted**

**Measurement Group:** Provisioning Performance

**Measurement**

**Type:** Simple

**Description:** The total number of SOAP transactions that have been successfully committed to the database.

**Collection Interval:** 5 min

**Peg Condition:** This measurement shall be incremented each time a SOAP transaction has been successfully committed to the database.

**Measurement Scope:** All

**Recovery:**

No action required.
<table>
<thead>
<tr>
<th>A</th>
<th>Application Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>A logical entity that hosts and executes services in an IMS network, interfacing</td>
</tr>
<tr>
<td></td>
<td>through SIP or a similar protocol.</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute-Value Pair</td>
</tr>
<tr>
<td></td>
<td>The Diameter protocol consists of a header followed by one or more attribute-value</td>
</tr>
<tr>
<td></td>
<td>pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific</td>
</tr>
<tr>
<td></td>
<td>data (e.g., routing information) as well as authentication, authorization or</td>
</tr>
<tr>
<td></td>
<td>accounting information.</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input-Output System</td>
</tr>
<tr>
<td></td>
<td>Firmware on the CPU blade that is executed prior to executing an OS.</td>
</tr>
<tr>
<td>CAPM</td>
<td>Computer-aided policy making</td>
</tr>
<tr>
<td>CMOS</td>
<td>Complementary Metal Oxide Semiconductor</td>
</tr>
<tr>
<td></td>
<td>CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity)</td>
</tr>
<tr>
<td></td>
<td>circuits. Since only one of the circuit types is on at any given time, CMOS chips</td>
</tr>
<tr>
<td></td>
<td>require less power than chips using just one type of transistor.</td>
</tr>
</tbody>
</table>
Communication Agent

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.

CPU

Central Processing Unit

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).

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

DEA

Diameter Edge Agent

Device through which LTE roaming signaling traffic is funneled to protect network.
### Glossary

**D**

- **element addresses from being exposed to third parties.**

**Diameter**

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.

**DNS**

Domain Name System

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

**DSR**

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.

**E**

**ESPR**

Enhanced Subscriber Profile Repository - Oracle Communications’ database system that provides the storage and management of subscriber policy control data for PCRF nodes.

**ETG**

Egress Throttle Group (s)
**FIPS**  
Federal Information Processing Standard

**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.

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

**HIDS**  
Host Intrusion Detection System

**HP**  
Hewlett-Packard

**IDIH**  
Integrated Diameter Intelligence Hub

**IMSI**  
International Mobile Subscriber Identity

**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.

KPI  Key Performance Indicator

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.

MSISDN  Mobile Station International Subscriber Directory Number. The unique, network-specific subscriber number of a mobile communications subscriber. MSISDN follows the E.164 numbering plan; that is, normally the MSISDN is the phone number that is used to reach the subscriber.

NAI  Nature of Address Indicator

A standard method of identifying users who request access to a network.

NS  Notification subscription

A subscription request made by a specific Subscribing Client to a specific subscriber public identity. It contains a list of the subscribed to Entity Alias values, the expiry time of the subscription, and
associated flags. It also contains information necessary to build and send a Notification to the Subscribing Client. This is stored as an entry in the individual’s SNO record object.

NTP

Network Time Protocol

NTP daemon

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

OAM

Operations, Administration, and Maintenance

The application that operates the Maintenance and Administration Subsystem that controls the operation of many products.

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

PCRF

Policy and Charging Rules Function
P

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

PNA
Push-Notification-Answer
Sent by a client in response to the Push-Notification-Request command.

PNR
Push Notification Request on Sh Interface
Sent by a Diameter server to a Diameter client in order to notify changes in the user data in the server.

PUA
Profile-Update-Answer
Command sent by a client in response to the Profile-Update-Request command.

PUR

R

RAS
REST Application Server

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

REPL
Replication

S
SCTP
Stream Control Transmission Protocol
SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

SDO
Subscription Data Object
An SDO consists of subscription state information and a collection of registers for storing entities. An individual SDO applies to one subscriber. A pool SDO applies to a group of subscribers.

SNA
Subscribes Notification Answer on Sh Interface

SNO
Subscription Notification Object.
An SNO stores a collection of client subscribe-to-notifications for a subscription.

SNMP
An industry-wide standard protocol used for network management. The SNMP agent
S

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.

SNR

Subscriber Notification Request on Sh Interface

SO

Signaling OAM

A server that manages a collection of MPs. SO servers are deployed in active/standby pairs.

SOAM

System Operations, Administration, and Maintenance

SOAP

Simple Object Access Protocol

split brain

Event where multiple active servers have been detected in the same cluster.

SQL

Structured Query Language

A special programming language for querying and managing databases.

SW

Software

UDA

User-Data-Answer

Sent by a server in response to the User-Data-Request command.
<table>
<thead>
<tr>
<th>UDR</th>
<th>User Data Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDRFE</td>
<td>UDR Front End</td>
</tr>
<tr>
<td>XSAS</td>
<td>XML SOAP Application Server</td>
</tr>
</tbody>
</table>