Oracle®Communications

User Data Repository

Alarms, KPIs, and Measurements Reference

Release 12.11.0

F56866-01

May 2022

ORACLE

Oracle Communications User Data Repository Alarms, KPIs, and Measurements Reference, Release 12.11.0

F56866-01

Contents

List of Figures

List of Tables

1

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.

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

- Information relevant to understanding alarms and events that may occur on the application
- List of alarms
- Information relevant to understanding Key Performance Indicators (KPIs) in the application
- List of KPIs
- Information relevant to understanding measurements in the application
- Measurement report elements
- List of measurements by function

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 Oracle Communications User Data Repository (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 User Data Repository 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 User Data Repository. For example, DSR applications (such as RBAR, FABR, CPA, and Policy DRA) and IPFE are currently not used by User Data Repository, 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, and how to Locate Product Documentation on the Oracle Help Center 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.

Locate Product Documentation on the Oracle Help Center Site

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

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support

My Oracle Support is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support 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 My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective

action. Critical situations affect service and/or system operation resulting in one or several of these situations:

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

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

2

User Interface Introduction

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 2-1 describes elements of the user interface.

Table 2-1 User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	The left side of the banner provides the following information: • Displays the company name, • product name and version, and • the alarm panel. The right side of the banner: • Allows you to pause any software updates. • Links to the online help for all software. • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • 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 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 Login Message.
Session Banner	Across the bottom of the web page	The left side of the banner provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The **HA** state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner shows the alarm panel.

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 2-2 Main Menu Options

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

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
UDR	Allows you to configure options for the UDR, UDRBE, 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 the password upon login. The System Login page also features a date and time stamp reflecting the time the page was last refreshed. Additionally, a customizable login message appears just below the **Log In** button.

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 to gain access.

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 2-1 Oracle System Login

1. From the **Main Menu**, click **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 displays.

Supported Browsers

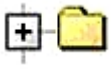
This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details

Main Menu Icons

This table describes the icons used in the Main Menu.

Table 2-3 Main Menu Icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Task	Contains operations related to Tasks
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

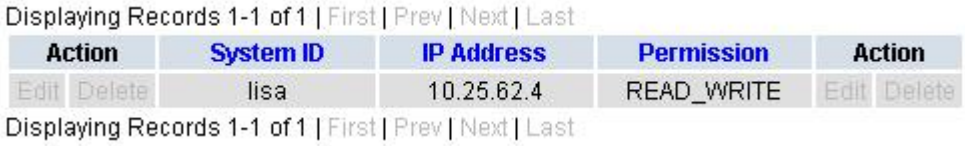
In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

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

Tables

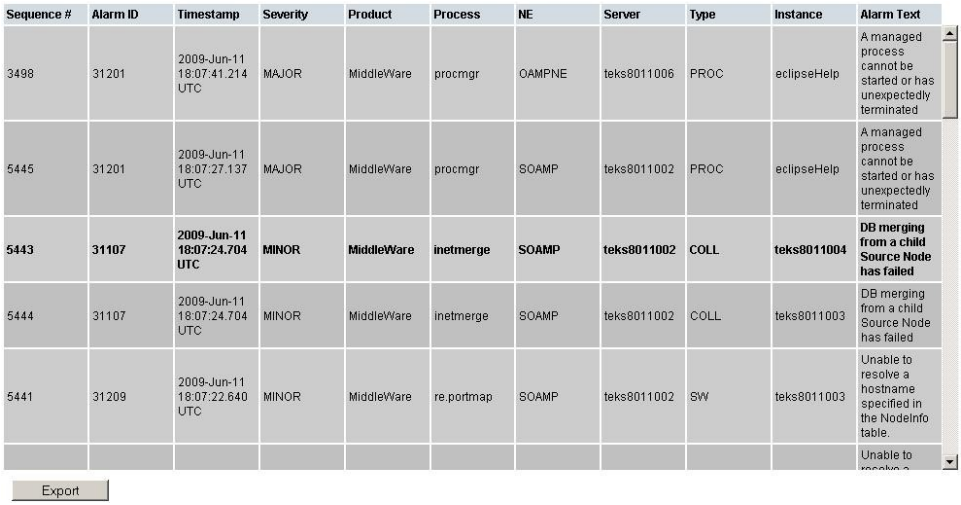
Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end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

Figure 2-2 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 2-3 Scrollable Table

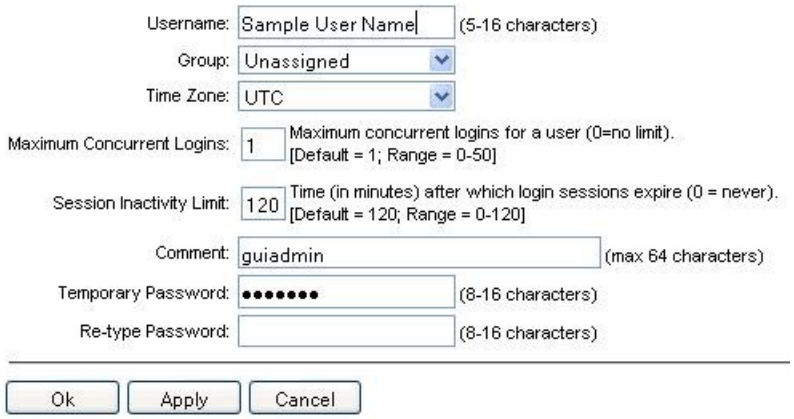


> **Note:** Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

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 lists, buttons, and links.

Figure 2-4 Form Page



Tabbed pages

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

Figure 2-5 Tabbed Pages

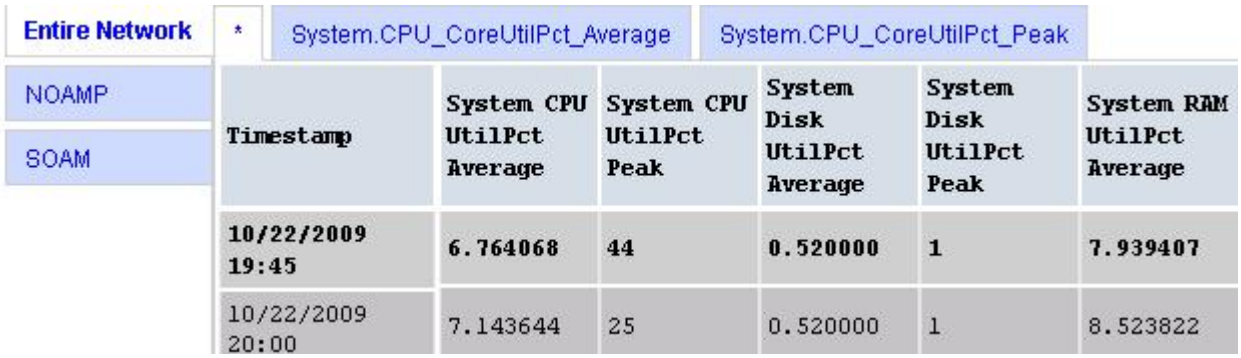
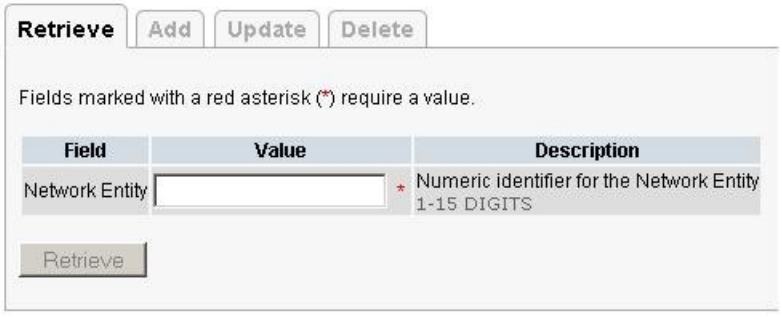


Figure 2-6 Tabbed Pages



Reports

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

Figure 2-7 Report Output

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

User Account Usage Report

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

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

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

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

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

End of User Account Usage Report

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

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the splash page appears. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Locate **Welcome Message** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.

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

The next time you log in to the user interface, the new 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.

Figure 2-8 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 2-4 contains examples of Action buttons.

Table 2-4 Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in Table 2-5, 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.

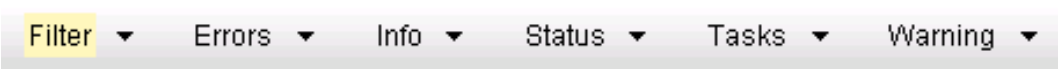
Table 2-5 Submit Buttons

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

Optional Layout Element Toolbar

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

Figure 2-9 Optional Layout Element Toolbar



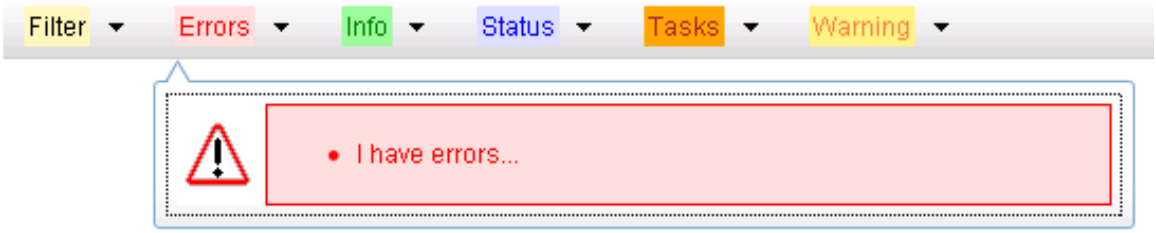
The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear include:

- 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.

Figure 2-10 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.

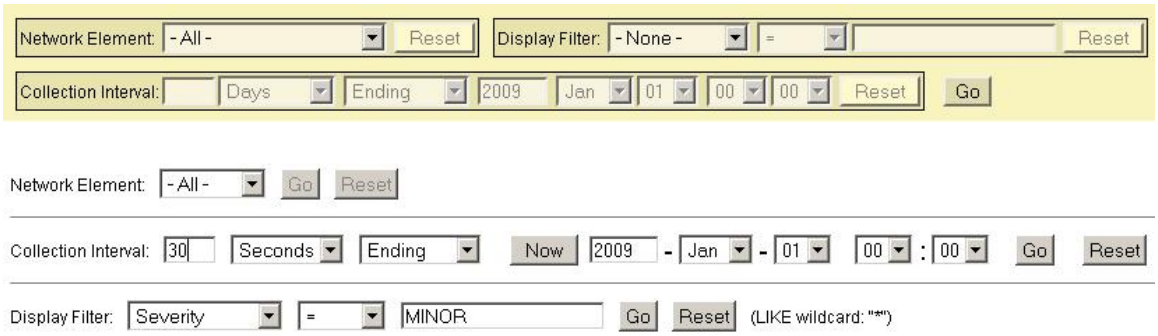
> **Note:** Once enabled, the Network Element filter affect all pages that list or display data relating to the Network Element.

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

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

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

Figure 2-11 Examples of Filter Styles



Filter Control Elements

This table describes filter control elements of the user interface.

Table 2-6 Filter Control Elements

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

Note: Not all filterable fields support all operators. Only the supported operators are 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.
2. Select a Network Element from the **Network Element** list.
3. Click **Go** to filter on the selection or click **Reset** to clear the selection.
4. For data tables that support compound filtering, click **Add** to add another filter condition and repeat steps 2 through 4.

   Multiple filter conditions are joined by an AND operator.

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.
2. Enter a duration for the **Collection Interval** filter.

   The duration must be a numeric value.
3. Select a unit of time from the list.

   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the list.
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 with the Display Filter field. This process is the same for all data tables. However, all filtering operations are not available for all tables.

Note: Display Filter does not support compound filtering. For example, you cannot filter on both severity and a server name. Try to filter on a single filter criteria, such as the server hostname for server-scoped metric cells; or the application name for St- and NE-scoped metric cells. You can also sort by congestion level (descending) to help improve your filter.

1. Click **Filter** in the optional layout element toolbar.
2. Select a field name from the **Display Filter** list.

   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.
3. Select an operator from the operation selector list.
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.

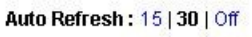
Records are displayed according to the specified criteria.

Note: PCA was known as PDRA and may still be seen in some filtering.

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**, click **Administration** > **General Options**.
2. Change the value of the **MaxRecordsPerPage** variable.

   Note: **Maximum Records Per Page** 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.

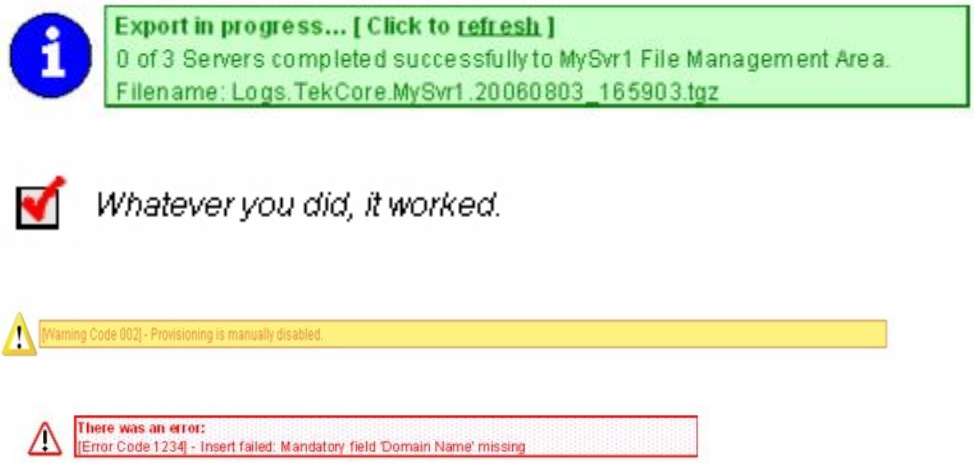
Apply saves the change and remains on the same page.

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:



3

Alarms and Events

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 and types of alarms/events.

Alarms and events defined

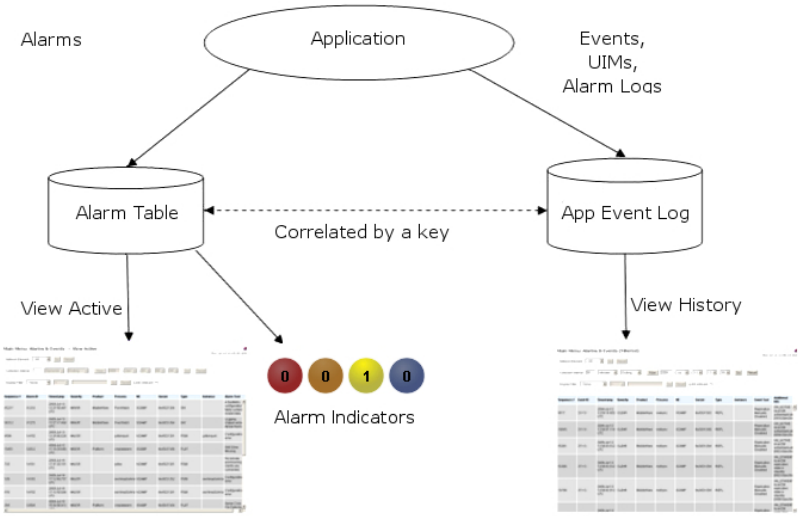
Alarms provide information pertaining to a system's operational condition that a network manager may need to act upon. An alarm might represent a change in an external condition, for example, a communications link has changed from connected to a disconnected state. Alarms can have these severities:

- Critical
- Major
- Minor
- Cleared — An alarm is considered inactive once it has been cleared, and cleared alarms are logged on the **Alarms & Events** > **View History** page.

Events note the occurrence of an expected condition, such as an unsuccessful login attempt by a user. Events have a severity of Info and are logged on the View History page.

Figure 3-1 shows how alarms and events are organized in the application.

Figure 3-1 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. This is shown in Figure 3-2 and Figure 3-3.

Figure 3-2 Alarm Indicators Legend

	Active Critical Alarm (bright red)
	Active Major Alarm (bright orange)
	Active Minor Alarm (bright yellow)
	No active Critical Alarm (pale red)
	No active Major Alarm (pale orange)
	No active Minor Alarm (pale yellow)
	Not Connected (white)

Figure 3-3 Trap Count Indicator Legend

	Trap count > 0 (bright blue)
	Trap count = 0 (pale blue)

Alarms 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 3-2.
- 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
- Alarm ID: alarm identifier used internally (may appear for some Platform alarms)
- 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 3-1 Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
Diameter	8000-8999
Operations, Administration, and Maintenance (**OAM**)	10000-10999
Provisioning (PROV) (UDR **RAS**, **XSAS**, and Prov-Misc)	13000-13100
User Data Repository (UDR)	13101-13500
Transport Manager	19000-19499
Communication Agent (**ComAgent**)	19800-19899
EXG Stack	19900-19999
Diameter	22000-22999

Table 3-1 (Cont.) Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
OAM Alarm Management	25500-25899
Platform	31000-32700

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 3-2 Alarm and Event Types

Type Name	Type
AUD	Audit
AUTH	Authorization
CAF	**Communication Agent** (**ComAgent**)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
COLL	Collection
DB	Database
DIAG	Diagnostic
DIAM	Diameter
DISK	Disk
HA	High Availability
IDIH	Integrated Diameter Intelligence Hub
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOG	Logging
MEAS	Measurements
MEM	Memory
OAM	Operations, Administration & Maintenance
PDRA	Policy DRA
PLAT	Platform

Table 3-2 (Cont.) Alarm and Event Types

Type Name	Type
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/UDRFE	UDR Front End Application running on MP Server

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.

8000-8999 Diameter

This section provides information and recovery procedures for Diameter alarms and events, 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.

8000 - MpEvFsmException

8000 - 001 - MpEvFsmException_SocketFailure

Event Type:
DIAM

Description:
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. This event is potentially caused by the DSR process reaching its descriptor capacity.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 002 - MpEvFsmException_BindFailure

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes of this event are:
   - Network interface(s) are down.
   - Port is already in use by another process.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 003 - MpEvFsmException_OptionFailure

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:003

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes of this event are:
   - DSR process is not running with root permission.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 004 - MpEvFsmException_AcceptorCongested

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:004

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. This event is potentially caused by a network or upgrade event that resulted in a synchronization of peer connection attempts.

Note: The rate will ease over time as an increasing number of connections are accepted.

8000 - 101 - MpEvFsmException_ListenFailure

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 102 - MpEvFsmException_PeerDisconnected

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. No action required.

8000 - 103 - MpEvFsmException_PeerUnreachable

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:103

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes for this event are:
   - A host IP interface is down.
   - A host IP interface is unreachable from the peer.
   - A peer IP interface is down.
   - A peer IP interface is unreachable from the host.

8000 - 104 - MpEvFsmException_CexFailure

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:104

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes for this event are:
   - The peer is misconfigured.
   - The host is misconfigured.

8000 - 105 - MpEvFsmException_CerTimeout

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:105

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. No action required.

8000 - 106 - MpEvFsmException_AuthenticationFailure

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:106

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes for this event are:
   - The peer is misconfigured.
   - The host is misconfigured.

8000 - 201 - MpEvFsmException_UdpSocketLimit

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery:

1. The DSR supports to a preconfigured maximum number of open UDP sockets (the maximum number of open UDP sockets can be accessed via **Diameter** > **Configuration** > **System Options** > **Maximum Open RADIUS UDP sockets per DA-MP**). One or more peers are being routed more traffic than is normally expected, or the peers are responding slowly, causing more than the usual number of UDP sockets being opened. The concerned peer can be identified using the reported connection ID. Investigate the reason for higher than normal traffic being forwarded to the peer, or why the peer is slow to respond.

8001 - MpEvException

8001 - 001 - MpEvException_Oversubscribed

Event Type
DIAM

Description
DA-MP exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterMpEvException

Recovery

1. Bounce one or more floating connections to force their migration to another DA-MP with available capacity.

8002 - MpEvRxException

8002 - 001 - MpEvRxException_DiamMsgPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. Potential causes of this event are:

   - One or more DA-MPs are unavailable and traffic has been distributed to the remaining DA-MPs.

- One or more peers are generating more traffic than is nominally expected.
- There are an insufficient number of DA-MPs provisioned.
- One or more peers are answering slowly, causing a backlog of pending transactions.

8002 - 002 - MpEvRxException_MaxMpsExceeded

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is potentially caused when a peer is generating more traffic than is nominally expected.

8002 - 003 - MpEvRxException_CpuCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:003

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. Potential causes for this event are:
   - One or more peers are generating more traffic than is nominally expected.
   - Configuration requires more CPU for message processing than is nominally expected.
   - One or more peers are answering slowly, causing a backlog of pending transactions

8002 - 004 - MpEvRxException_SigEvPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:004

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 005 - MpEvRxException_DstMpUnknown

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:005

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 006 - MpEvRxException_DstMpCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:006

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. Potential causes for this event are:
   - One or more peers are generating more traffic than is nominally expected.
   - Configuration requires more CPU for message processing than is nominally expected.
   - One or more peers are answering slowly, causing a backlog of pending transactions.

8002 - 007 - MpEvRxException_DrlReqQueueCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:007

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 008 - MpEvRxException_DrlAnsQueueCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:008

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 009 - MpEvRxException_ComAgentCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:009

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 201 - MpEvRxException_MsgMalformed

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8002 - 202 - MpEvRxException_PeerUnknown

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. The host or peer may be misconfigured. Adjust the peer IP address(es) option of the associated Peer Node if necessary.

8002 - 203 - MpEvRxException_RadiusMsgPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

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. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 204 - MpEvRxException_ItrPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery:

1. Adjust the RADIUS **Cached Response Duration** option of the associated Connection configuration set(s) to reduce the lifetime of cached transactions, if needed.
2. 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.
3. 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.
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 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.
5. 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.

6. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 205 - MpEvRxException_RclRxTaskQueueCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery:

1. The alarm will clear when the DCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 206 - MpEvRxException_RclSigEvPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:206

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

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, it is recommended to contact My Oracle Support.

8002 - 207 - MpEvRxException_ReqDuplicate

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:207

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery:

1. It is possible to observe this event occasionally, due to the unreliable nature of the UDP transport protocol. However, if the occurrence of this event is frequent, investigate the issue further.

   This event is expected when a retransmission is received from the client before a server has responded to the request, possibly a result of the client retransmitting too quickly before allowing sufficient time for a server to respond in time. Another possible cause is if one or more servers configured to handle the request are non-responsive.

2. Investigate the routing configuration to narrow down the list of servers (Peer Nodes) which are expected to handle requests from the reported server connection.
3. Evaluate whether an Egress Transaction Failure Rate alarm has been raised for any of the corresponding client connections. If so, investigate the cause of the server becoming non-responsive and address the condition.

> **Note:** Depending on the operator's choice, the client connection may need to be Admin Disabled until the evaluation is complete, which will allow requests to be routed to other servers, depending on the routing configuration. If this is not the case, tune the client's retransmit timers to be greater than the typical turnaround time for the request to be processed by the server and for the response to be sent back to the client.

4. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 208 - MpEvRxException_SharedSecretUnavailable

Event Type
DIAM

Description
Failed to access shared secret.

Severity
Info

Instance
<Connection Name>:208

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery:

1. Check to see if alarm 8207 is present. If so, follow the recovery steps for alarm 8207 - MpRadiusKeyError.

8003 - MpEvTxException

8003 - 001 - MpEvTxException_ConnUnknown

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery

1. No action required.

8003 - 101 - MpEvTxException_DclTxTaskQueueCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery

1. This event is potentially caused by one or more peers being routed more traffic than is nominally expected.

8003 - 201 - MpEvTxException_RclTxTaskQueueCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery:

1. The alarm will clear when the DCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8003 - 202 - MpEvTxException_EtrPoolCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery:

1. Adjust the Diameter **Pending Answer Timer** option of the associated Transaction configuration set(s) to reduce the lifetime of pending transactions, if needed.
2. 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.
3. 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.

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 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.
5. 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.
6. If the problem persists, it is recommended to contact My Oracle Support.

8003 - 203 - MpEvTxException_RadiusMsgPoolCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

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. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8003 - 204 - MpEvTxException_RadiusIdPoolCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery:

1. The peer is being routed more traffic than is nominally expected, or is responding slowly. If the problem persists, the client port range configured in the Local Node corresponding to the indicated transport connection may need to be increased.
2. Access the connection information via **Diameter** > **Configuration** > **Connections** screen, which indicates the associated Local Node.
3. Access the Local Node screen via **Diameter** > **Configuration** > **Local Nodes**.
4. Update the client port range by modifying the **RADIUS Client UDP Port Range Start** and the **RADIUS Client UDP Port Range End** values in the Local Node edit screen, if necessary.

> **Note:** To update the Local Node configuration, Admin Disable all associated connections.

8003 - 205 - MpEvTxException_SharedSecretUnavailable

Event Type
DIAM

Description
Failed to access shared secret.

Severity
Info

Instance
<DA-MP Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery:

1. Proceed to 2 if alarm 8207 - MpRadiusKeyError is present.
2. Synchronize the RADIUS key file.
3. Restart the DSR process. If the required keys are now available, the alarm will not be raised.
4. If the problem persists, it is recommended to contact My Oracle Support.

8004 - EvFsmAdState

8004 - 001 - EvFsmAdState_StateChange

Event Type
DIAM

Description
Connection FSM administrative state change.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterEvFsmAdState

Recovery

1. No action required.

8005 - EvFsmOpState

8005 - 001 - EvFsmOpState_StateChange

Event Type
DIAM

Description
Connection FSM operational state change.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterFsmOpState

Recovery

1. No action required when operationally available.
2. Potential causes for this event when operationally unavailable are:
   - Connection is administratively disabled.
   - Diameter initiator connection is connecting.
   - Diameter initiator connection is suppressed (peer is operationally available).
   - Diameter initiator connection is suppressed (peer did not signal reboot during graceful disconnect).
   - Diameter responder connection is listening.
   - RADIUS server connection is opening.
3. Potential causes for this event when operationally degraded are:
   - Connection egress message rate threshold crossed.
   - Diameter connection is in watchdog proving.
   - Diameter connection is in graceful disconnect.
   - Diameter peer signaled remote busy.
   - Diameter connection is in transport congestion.

8006 - EvFsmException

8006 - 001 - EvFsmException_DnsFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes of this event are:
   - DNS server configuration is invalid.
   - DNS server(s) are unavailable.
   - DNS server(s) are unreachable.
   - FQDN configuration is invalid.

8006 - 002 - EvFsmException_ConnReleased

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. No action required.

8006 - 101 - EvFsmException_SocketFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. This event is potentially caused by the DSR process reaching its descriptor capacity.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 102 - EvFsmException_BindFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:
   - Network interface(s) are down.
   - Port is already in use by another process.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 103 - EvFsmException_OptionFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:103

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:
   - DSR process is not running with root permission.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 104 - EvFsmException_ConnectFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:104

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 105 - EvFsmException_PeerDisconnected

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:105

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. No action required. Potential causes for this event are:
   - Diameter peer signaled **DPR**.
   - Peer is unavailable.

8006 - 106 - EvFsmException_PeerUnreachable

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:106

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:
   - A host IP interface is down.
   - A host IP interface is unreachable from the peer.
   - A peer IP interface is down.
   - A peer IP interface is unreachable from the host.

8006 - 107 - EvFsmException_CexFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:107

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:
   - The peer is misconfigured.
   - The host is misconfigured.

8006 - 108 - EvFsmException_CeaTimeout

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:108

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. No action required.

8006 - 109 - EvFsmException_DwaTimeout

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:109

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. No action required.

8006 - 110 - EvFsmException_DwaTimeout

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:110

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. No action required.

8006 - 111 - EvFsmException_ProvingFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:111

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:

- A host IP interface is unreachable from the peer, or intermittently so.
- A peer IP interface is unreachable from the host, or intermittently so.

8006 - 112 - EvFsmException_WatchdogFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:112

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:
   - A host IP interface is unreachable from the peer, or intermittently so.
   - A peer IP interface is unreachable from the host, or intermittently so.

8006 - 113 - EvFsmException_AuthenticationFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:113

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

Recovery

1. Potential causes for this event are:
   - The peer is misconfigured.
   - The host is misconfigured.

8007 - EvException

8007 - 101 - EvException_MsgPriorityFailure

Event Type
DIAM

Description
Connection exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvException

Recovery

1. This event is potentially caused by misconfiguration of the host.

8008 - EvRxException

8008 - 001 - EvRxException_MaxMpsExceeded

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery

1. This event is potentially caused when a peer is generating more traffic than is nominally expected.

8008 - 101 - EvRxException_MsgMalformed

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8008 - 102 - EvRxException_MsgInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8008 - 201 - EvRxException_SharedSecretUnavailable

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 202 - EvRxException_MsgAttrLenUnsupported

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 203 - EvRxException_MsgTypeUnsupported

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect or may be misconfigured.

8008 - 204 - EvRxException_AnsOrphaned

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. The peer is responding slowly, network latency is high, or the ETR timer is configured too small. Adjust the Diameter **Pending Answer Timer** option of the associated Transaction configuration set(s) to reduce the lifetime of pending transactions, if needed.

8008 - 205 - EvRxException_AccessAuthMissing

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 206 - EvRxException_StatusAuthMissing

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:206

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 207 - EvRxException_MsgAuthInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:207

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. Evaluate the indicated message. If an invalid message authenticator value is indicated, ensure that the same shared secret is configured for the connection on the DSR and on the RADIUS peer. The shared secret configuration set associated with the transport connection on the DSR can be accessed via **Diameter** > **Configuration** > **Connections**.
2. If an invalid message authenticator value is not indicated, then the peer may have an implementation defect or may be misconfigured. It is recommended to contact My Oracle Support for assistance. This event is unexpected.

8008 - 208 - EvRxException_ReqAuthInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:208

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.

8008 - 209 - EvRxException_AnsAuthInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:209

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.

8008 - 210 - EvRxException_MsgAttrAstUnsupported

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:210

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect or may be misconfigured .
2. Only certain Acct-Status-Type values are supported. Ensure that the Acct-Status-Type value is one of these values:
   - 1 (Start)
   - 2 (Stop)
   - 3 (Interim-Update)
   - 7 (Accounting-On)
   - 8 (Accounting-Off)

8008 - 212 - EvRxException_MsgTypeMissingMccs

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:212

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. It is recommended to contact My Oracle Support for assistance. The peer or host is misconfigured.

8008 - 213 - EvRxException_ConnUnavailable

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:213

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

Recovery:

1. No action required. This event is for informational purposes only.

8009 - EvTxException

8009 - 001 - EvTxException_ConnUnavailable

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery

1. No action required.

8009 - 101 - EvTxException_DclTxConnQueueCongested

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery

1. This event is potentially caused by a peer being routed more traffic than is nominally expected.

8009 - 102 - EvTxException_DtlsMsgOversized

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery

1. This event is potentially caused by a peer being routed more traffic than is nominally expected.

8009 - 201 - EvTxException_MsgAttrLenUnsupported

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8009 - 202 - EvTxException_MsgTypeUnsupported

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect, or may be misconfigured.

8009 - 203 - EvTxException_MsgLenInvalid

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.
2. This event is typically generated when the DSR needs to add a Message-Authenticator to the message, but doing so causes the message size to exceed maximum RADIUS message length. If this problem persists, evaluate the source of this message and ensure that the message size allows adding a Message-Authenticator attribute (16 octets). Evaluate the message authenticator configuration for the egress connection and ensure that the adding of Message-Authenticator to specific message types is configured appropriately. The message authenticator configuration set can be identified by accessing the connection screen via **Diameter** > **Configuration** > **Connections**.

8009 - 204 - EvTxException_ReqOnServerConn

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Review the configuration of Route Groups and ensure that there are no RADIUS server instances.

8009 - 205 - EvTxException_AnsOnClientConn

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Review the configuration of Connections and ensure that there are no RADIUS client instances being used as a RADIUS server by one or more peers.

8009 - 206 - EvTxException_DiamMsgMisrouted

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:206

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Review the configuration of Route Groups and ensure that there are no RADIUS server instances.

8009 - 207 - EvTxException_ReqDuplicate

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:207

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. No action required.

8009 - 208 - EvTxException_WriteFailure

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:208

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

Recovery:

1. This event is unexpected. It is recommend to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Ensure that the RADIUS **UDP Transmit Buffer Size** option in System Options to ensure it is sufficient for the offered traffic load.

8010 - MpIngressDrop

Alarm Group
DIAM

Description
DA-MP ingress message discarded or rejected.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpIngressDrop

Recovery

1. Potential causes of this alarm are:

- One or more DA-MPs are unavailable and traffic has been distributed to the remaining DA-MPs.
- One or more peers are generating more traffic than is nominally expected.
- There are an insufficient number of DA-MPs provisioned.
- One or more peers are answering slowly, causing a backlog of pending transactions.

8011 - EcRate

Alarm Group
DIAM

Description
Connection egress message rate threshold crossed.

Severity
Minor, Major, Critical

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterEmr

Recovery

1. This alarm is potentially caused when a peer is routed more traffic than is nominally expected.

8012 - MpRxNgnPsOfferedRate

Alarm Group
DIAM

Description
DA-MP ingress NGN-PS message rate threshold crossed.

Severity
Major

Instance
MpRxNgnPsOfferedRate, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRxNgnPsOfferedRateNotify

Recovery

1. Potential causes of this alarm:

   - One or more DA-MPs are unavailable and traffic has been distributed to the remaining DA-MPs.
   - One or more peers are generating more traffic than is nominally expected.
   - There are an insufficient number of DA-MPs provisioned.

   The alarm will clear when threshold crossing abates.

8013 - MpNgnPsStateMismatch

Alarm Group
DIAM

Description
DA-MP NGN-PS administrative and operational state mismatch.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpNgnPsStateMismatchNotify

Recovery

1. This alarm is potentially caused when a DA-MP restart is required.

   The alarm will clear when administrative and operational states are aligned.

8014 - MpNgnPsDrop

Alarm Group
DIAM

Description
DA-MP NGN-PS message discarded or rejected.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpNgnPsDropNotify

Recovery

1. Potential causes of this alarm are:

   - Routing or application controls are configured incorrectly.
   - Peer or network is in congestion.
   - Engineering of internal resources is insufficient.

8015 - NgnPsMsgMisrouted

Alarm Group
DIAM

Description
NGN-PS message routed to peer DSR lacking NGN-PS support.

Severity
Major

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterNgnPsMsgMisroutedNotify

Recovery

1. Potential causes of this alarm are:

   - Routing configuration is incorrect.
   - Peer **DSR** has not yet been upgraded.

- Peer **DSR** has not yet operationally enabled NGN-PS.

8100 - NormMsgMisrouted

Alarm Group:
DIAG

Description:
Normal message routed onto diagnostic connection.

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
30 (after last occurrence)

OID:
eagleXgDiameterNormMsgMisrouted

Recovery:

1. The alarm is potentially caused by a diameter routing misconfiguration.
2. If the problem persists, it is recommended to contact My Oracle Support.

8101 - DiagMsgMisrouted

Alarm Group:
DIAG

Description:
Diagnostic message routed onto normal connection.

Severity:
Minor

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
30 (after last occurrence)

OID:
eagleXgDiameterDiagMsgMisrouted

Recovery:

1. The alarm is potentially caused by a diameter routing misconfiguration.
2. If the problem persists, it is recommended to contact My Oracle Support.

8200 - MpRadiusMsgPoolCongested

Alarm Group
DIAM

Description
DA-MP RADIUS message pool utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
MpRadiusMsgPool, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRadiusMsgPoolCongested

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, it is recommended to contact My Oracle Support.

8201 - RclRxTaskQueueCongested

Alarm Group
DIAM

Description
RCL ingress task message queue utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
RclRxTaskQueue, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclRxTaskQueueCongested

Recovery:

1. The alarm will clear when the RCL ingress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8202 - RclItrPoolCongested

Alarm Group
DIAM

Description
RCL ITR pool utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
RclItrPool, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclItrPoolCongested

Recovery:

1. Adjust the RADIUS **Cached Response Duration** option of the associated Connection configuration set(s) to reduce the lifetime of cached transactions, if needed.
2. 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.

3. 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.
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 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.
5. 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.
6. If the problem persists, it is recommended to contact My Oracle Support.

8203 - RclTxTaskQueueCongested

Alarm Group
DIAM

Description
RCL egress task threshold crossed.

Severity
Minor, Major, Critical

Instance
RclTxTaskQueue, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclTxTaskQueueCongested

Recovery:

1. The alarm will clear when the RCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8204 - RclEtrPoolCongested

Alarm Group
DIAM

Description
RCL ETR pool utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
RclEtrPool, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclEtrPoolCongested

Recovery:

1. Adjust the RADIUS **Cached Response Duration** option of the associated Connection configuration set(s) to reduce the lifetime of cached transactions, if needed.
2. 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.
3. 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.
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 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.
5. 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.
6. If the problem persists, it is recommended to contact My Oracle Support.

8205 - RadiusXactionFail

Alarm Group
DIAM

Description
RADIUS connection transaction failure threshold crossed. The presence of this alarm indicates that the server is not responding to requests in a timely manner. A response that is not received in a timely manner constitutes a transaction failure.

Severity
Minor, Major

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRadiusXactionFail

Recovery:

1. Check whether there is an IP network problem, RADIUS server congestion resulting in large response times, or whether a RADIUS server failure has occurred.
2. The user may choose to Admin Disable the corresponding transport connection which will prevent the **DSR** from selecting that connection for message routing, until the cause of the alarm is determined.

8206 - MpRxRadiusAllLen

Alarm Group
DIAM

Description
RADIUS average ingress message length threshold crossed.

Severity
Minor, Major

Instance
MpRxRadiusAllLen, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRxRadiusAllLen

Recovery:

1. Investigate traffic sources. One or more peers is sending larger messages than is nominally expected.
2. Adjust the message length thresholds if necessary.

8207 - MpRadiusKeyError

Alarm Group
DIAM

Description
DA-MP RADIUS key error. This alarm is unexpected during normal processing. The presence of this alarm indicates DSR encountered an error while accessing RADIUS encryption keys used to decrypt RADIUS shared secrets.

Severity
Critical

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRadiusKeyError

Recovery:

1. Synchronize the RADIUS key file.
2. Restart the DSR process. If the required keys are now available, the alarm is not raised.
3. If the problem persists, it is recommended to contact My Oracle Support.

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.

> **Note:** As of AppWorks 5.0, this alarm is no longer used.

Severity:
Critical

Instance:
N/A

HA Score:
Failed

Auto Clear Seconds:
300

OID:
tekelecIncompatibleDatabaseVersionNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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:

1. 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:

1. 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:

1. It is recommended to contact My Oracle Support.

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:

1. 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:

1. 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:

1. It is recommended to contact My Oracle Support.

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:
tekelecProvisioningManuallyDisabledNotify

Recovery:

1. 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. The 10009 alarm raises when DB re-initialization is attempted but fails. The re-initialization usually happens when transitioning to 'A' state (one of the procmgr state, can get it from pl command). DB re-initialization fails because the remote server is not in the correct state, e.g., it is not in OOS state.

This alarm can also be observed during some DSR patch installation after the DB replication is inhibited. As long as this alarm is cleared (NOT stuck) after DB replication is allowed, it is normal behavior and we expect to see alarm 10009 when applying the patch.

Severity:
Critical

Instance:
N/A

HA Score:
Failed

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTCfgProvDbNoSyncNotify

Recovery:

1. Monitor the replication status by navigating to **Status & Manage** > **Replication GUI**.
2. If alarm persists for more than one hour, it is recommended to contact My Oracle Support.

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:
oAGTStDbNoSyncNotify

Recovery:

1. If alarm persists for more than 30 seconds, it is recommended to contact My Oracle Support.

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:
oAGTCantMonitorTableNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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:
oAGTResponderFailedNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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:
oAGTApplSWDisabledNotify

Recovery:

1. If duration of alarm is greater than two seconds, it is recommended to contact My Oracle Support.

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:
apwBackupFailureNotify

Recovery:

1. Alarm will clear if a backup (Automated or Manual) of the same group data is successful. It is recommended to contact My Oracle Support if failures persist.

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:

1. No action required.

10140 - Site Upgrade Started

Event Type:
LOG

Description:
Site upgrade operation started.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeStart

Recovery:

1. No action required.

10141 – Diameter Peer Config Fail

Message
Diameter: Peer Configuration Failure. *{0}*

Description
The specified Diameter Peer configuration failed.

Severity
Warning

Notification
Trace Log

Alarm
No

Trap
No

Server
MPE

Group
Diameter

Recovery

1. If the problem persists, contact My Oracle Support.

10142 - Site Upgrade Successful

Event Type:
LOG

Description:
Site upgrade operation completed successfully.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeSuccess

Recovery:

1. No action required.

10143 - Site Upgrade Failed

Event Type:
LOG

Description:
Site upgrade operation failed.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeFailed

Recovery:

1. No action required. Alarm 10134 - Server Upgrade Failed is raised for each server in the site that failed to upgrade. The alarm clears when the server upgrades successfully.

10144 - Site Upgrade Cancelled - User Request

Event Type:
LOG

Description:
Site upgrade cancelled by user.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeCancelledUser

Recovery:

1. No action required.

10050 - Resource Audit Failure

Alarm Group:
AUD

Description:
Database backup failed.

Severity:
Minor

Instance:

HA Score:
Normal

Auto Clear Seconds:
0

OID:
tekelecResourceAuditFailureNotify

Recovery:

1. If the problem persists, it is recommended to contact My Oracle Support.

10051 - Route Deployment Failed

Alarm Group:
AUD

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

Severity:
Minor

Instance:
Route ID that failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0

OID:
tekelecRouteDeploymentFailedNotify

Recovery:

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

10052 - Route discovery failed

Alarm Group:
AUD

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

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
tekelecRouteDiscoveryFailedNotify

Recovery:

1. If the problem persists, it is recommended to contact My Oracle Support.

10053 - Route deployment failed - no available device

Alarm Group:
AUD

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

Severity:
Minor

Instance:
Route ID that failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0

OID:
tekelecNoRouteDeviceNotify

Recovery:

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

10054 - Device deployment failed

Alarm Group:
AUD

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

Severity:
Minor

Instance:
Device name that failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0

OID:
tekelecDeviceDeploymentFailedNotify

Recovery:

1. Edit or delete the device.

10055 - Device discovery failed

Alarm Group:
AUD

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

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
tekelecDeviceDiscoveryFailedNotify

Recovery:

1. If the problem persists, it is recommended to contact My Oracle Support.

10073 - Server Group Max Allowed HA Role Warning

Alarm Group:
HA

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

Severity:
Minor

Instance:
Affected Server Group name

HA Score:
Normal

Auto Clear Seconds:
0

OID:
oAGTSgMaxAllowedHARoleWarnNotify

Recovery:

1. Log into the SO GUI and navigate to the HA page (**Main Menu** > **Status & Manage** > **HA**).
2. Click the **Edit** button and change the Max Allowed HA role of the current Standby SOAM to *Active*.
3. If you cannot perform the HA switchover, log into the server (**Main Menu** > **Status & Manage** > **Server**).
4. Click on the Active server and press the **Restart** button to restart the server.

   HA switchover occurs.
5. Verify the switchover was successful from the Active SOAM GUI, or login to the Active and Standby SOAMs and execute this command:

   ```
   # ha.mystate
   ```

10074 - Standby server degraded while mate server stabilizes

Alarm Group:
HA

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

Severity:
Minor

Instance:
N/A

HA Score:
Degraded

Auto Clear Seconds:
This alarm does not autoclear.

OID:
hASbyRecoveryInProgressNotify

Recovery:

1. 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:
Normal

Auto Clear Seconds:
This alarm does not clear automatically.

OID:
hAMtceStopApplicationsNotify

Recovery:

1. 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:
failureRecoveryWithoutAppRestartNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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:
tekelecLogExportStartNotify

Recovery:

1. 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:
tekelecLogExportSuccessNotify

Recovery:

1. 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:
tekelecLogExportFailedNotify

Recovery:

1. Verify the export request and try the export again.
2. If the problem persists, it is recommended to contact My Oracle Support.

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:
tekelecLogExportNotRunNotify

Recovery:

1. 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:
tekelecExportXferFailedNotify

Recovery:

1. It is recommended to contact My Oracle Support 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:
tekelecLogExportCancelledUserNotify

Recovery:

1. It is recommended to contact My Oracle Support 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:
tekelecLogExportCancelledDuplicateNotify

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, it is recommended to contact My Oracle Support 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:
tekelecLogExportCancelledQueueNotify

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, it is recommended to contact My Oracle Support 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:
tekelecLogExportDupSchedTaskNotify

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, it is recommended to contact My Oracle Support 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:
tekelecLogExportQueueFullNotify

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, it is recommended to contact My Oracle Support 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:

1. It is recommended to contact My Oracle Support 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:

1. It is recommended to contact My Oracle Support 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:

1. It is recommended to contact My Oracle Support for assistance.

10115 - Health Check Started

Event Type:
LOG

Description:
Upgrade health check operation started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckStart

Recovery:

1. No action required.

10116 - Health Check Successful

Event Type:
LOG

Description:
Upgrade health check operation completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckSuccess

Recovery:

1. No action required.

10117 - Health Check Failed

Event Type:
LOG

Description:
Upgrade health check operation failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckFailed

Recovery:

1. No action required.

10118 - Health Check Not Run

Event Type:
LOG

Description:
Upgrade health check not run.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckNotRun

Recovery:

1. It is recommended to contact My Oracle Support.

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:

1. 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:

1. 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:

1. 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:

1. No action required. Alarm 10134 - Server Upgrade Failed is raised for each server in the server group that failed to upgrade. The alarm clears when the server upgrades successfully.

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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required. Alarm 10134 - Server Upgrade Failed is raised for each server that failed to upgrade. The alarm clears when the server upgrades successfully.

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 a server upgrade fails, this alarm clears when the server upgrades successfully. Upgrade the server individually or as part of a server group or site upgrade. If

more than one server in the same server group or site fails to upgrade, the server group and site upgrades may be useful because both methods will attempt to upgrade all of the failed servers within the server group or site, respectively. Upgrading all servers in a server group is useful if the server group has multiple upgrade failures. Upgrading all servers in a site is useful if servers in multiple server groups contained in a site have upgrade failures.

2. To upgrade individual servers:

   a. Navigate to the Upgrade page (**Administration** > **Software Management** > **Upgrade**).

   b. To upgrade a NOAM server, select the NOAM tab and proceed to 2.e.

   c. To upgrade a server that is not a NOAM server, select the SOAM site tab associated with the server(s) that raised the alarm.

   d. Select the sub-tab associated with the server group containing the server(s) that raised the alarm.

   e. Select the individual server(s) and then click the **Upgrade Server** button to start the upgrade on the selected servers.

   Note: Servers cannot be selected across tabs. If there are servers in multiple server groups, you must restart the server upgrade for each additional Server Group tab, or perform a server group or site upgrade.

3. To upgrade all servers in a server group:

   a. Navigate to the Upgrade page (**Administration** > **Software Management** > **Upgrade**).

   b. To upgrade a NOAM server, select the NOAM tab and proceed to 3.e.

   c. To upgrade a server that is not a NOAM server, select the SOAM site tab associated with the server(s) that raised the alarm.

   d. Select the sub-tab associated with the server group containing the server(s) that raised the alarm.

   e. Click **Auto Upgrade** to upgrade all servers in the server group. (Do not select any servers.)

   Note: The active server in the NO server group will never upgrade automatically.

An alternative method to upgrade a server group that is not a NOAM server group is to upgrade selected server groups from the Entire Site sub-tab. The site upgrade form does not offer as many options as the automated server group upgrade.

To upgrade all servers in a server group using the alternative method:

a. Navigate to the Upgrade page (**Administration** > **Software Management** > **Upgrade**).

b. Select the SOAM site tab associated with the server(s) that raised the alarm. Remain on the Entire Site sub-tab.

Note: The Entire Site sub-tab only appears when the site contains more than one server group.

c. Select the individual server group(s) then click the **Upgrade Server Group** button to start the upgrade on the selected server group(s).

4. To upgrade entire sites:

a. Navigate to the Upgrade page (**Administration** > **Software Management** > **Upgrade**).

b. Select the SOAM site tab associated with the server(s) that raised the alarm. Remain on the Entire Site sub-tab.

Note: The Entire Site sub-tab only appears when the site contains more than one server group.

c. Click **Site Upgrade** to upgrade all server groups in the site. (Do not select any server groups.)

10151 - Login successful

Event Type:
LOG

Description:
The login operation was successful.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLoginSuccessNotify

Recovery:

1. 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:
tekelecLoginFailedNotify

Recovery:

1. 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:
tekelecLogoutSuccessNotify

Recovery:

1. 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:
tekelecAccountDisabledNotify

Recovery:

1. 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:
tekelecSamlLoginSuccessNotify

Recovery:

1. 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 it is recommended to contact My Oracle Support 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:
apwSgDbReinitNotify

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, it is recommended to contact My Oracle Support.

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.

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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:

1. 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, it is recommended to call My Oracle Support.

13012 - RAS Connection Denied

Alarm Type:
UDR

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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:

1. 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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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:
ProvImportGenerationFailed

Recovery:

1. Correct the problem based on the error in the trace log.
2. Try the import again.
3. If the problem persists, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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:

1. 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, it is recommended to call My Oracle Support.

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:
provexport

HA Score:
Normal

Auto Clear Seconds:
43200

OID:
ProvExportGenerationFailed

Recovery:

1. Correct the problem based on the error in the trace log.
2. Try the export again.
3. If the problem persists, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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:

1. 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:

1. It is recommended to call My Oracle Support.

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)

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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%
- 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:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)
2. If the problem persists, it is recommended to call My Oracle Support.

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:
   - <= 57% (clears Minor alarm)
   - <= 63% (clears Major alarm)
   - <= 69% (clears Critical alarm)
2. If the problem persists, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

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, it is recommended to call My Oracle Support.

13068 - Command Log Export Initialization Failed

Alarm Type:
PROV

Description:
Command Log Export failed due to an initialization error. Alarm clears automatically after 12 hours or when initialization completes successfully.

Severity:
Major

Instance:
cmdlogexport

HA Score:
Normal

Auto Clear Seconds:
43200

OID:
ProvCommandLogExportInitializationFailed

Recovery:

1. Correct the problem based on the error in the trace log and wait for the command log export to be triggered again.
2. If the problem persists, it is recommended to call My Oracle Support.

13069 - Command Log Export Generation Failed

Alarm Type:
PROV

Description:
Command Log Export failed due to a failure in generating the command log export.

Severity:
Major

Instance:
cmdlogexport

HA Score:
Normal

Auto Clear Seconds:
43200

OID:
ProvCommandLogExportGenerationFailed

Recovery:

1. Correct the problem based on the error in the trace log and wait for the command log export to be triggered again.
2. If the problem persists, it is recommended to call My Oracle Support.

13070 - Command Log Export Transfer Failed

Alarm Type:
PROV

Description:
Command log export failed due to a file transfer error of command log export log. This alarm is raised when there are wrong or missing credentials, or the disk is full on the remote server.

Severity:
Major

Instance:
cmdlogexport

HA Score:
Normal

Auto Clear Seconds:
43200

OID:
ProvCommandLogExportTransferFailed

Recovery:

1. Correct the problem based on the error in the trace log and wait for the command log export to be triggered again.
2. If the problem persists, it is recommended to call My Oracle Support.

13071 - No Northbound Provisioning Connections

Alarm Type:
PROV

Description:
Alarm occurs when OCUDR is started and there are no active SOAP or REST connections from a remote provisioning system, or when the last active SOAP or REST provisioning connection is disconnected.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
86400

OID:
ProvNoRemoteConnections

Recovery:

1. Check that the provisioning system is attempting to establish a SOAP or REST connection, and verify the TCP/IP connectivity between the provisioning system and OCUDR.
2. View the whitelist from the Provisioning Connections GUI option on the UDR Configuration menu. Ensure that the IP address of the provisioning system has been added to the IP whitelist of allowed provisioning clients.
3. If the problem persists, it is recommended to call My Oracle Support.

13075 - Provisioning Interfaces Disabled

Alarm Type:
PROV

Description:
Alarm occurs when UDR is started and both the SOAP and the REST interfaces are disabled. Since both SOAP and REST interfaces are disabled by default when UDR is newly installed, this alarm is automatically generated on installation.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
86400

OID:
ProvInterfaceDisabled

Recovery:

1. Use the Provisioning Connections GUI page on the UDR Configuration menu to make sure a SOAP/REST provisioning connection exists.
2. Manually enable the SOAP and/or the REST interface on the Provisioning Options GUI page on the UDR Configuration menu.

   The alarm should clear.
3. If the problem persists, it is recommended to call My Oracle Support.

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:

1. It is recommended to contact My Oracle Support for assistance if needed.

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:

1. It is recommended to contact My Oracle Support for assistance if needed.

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

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMAeProvCreateFailed

Recovery:

1. It is recommended to contact My Oracle Support for assistance if needed.

13154 - AE Convert Failed

Alarm Type:
UDR

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMAeConvertToProvFailed

Recovery:

1. It is recommended to contact My Oracle Support for assistance if needed.

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:
Major

Instance:
Info

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
QuotaResetActivityStarted

Recovery:

1. No action required.

13156 - Scheduled Quota Reset Activity completed

Alarm Type:
UDR

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
QuotaResetActivityCompleted

Recovery:

1. No action required.

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

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
QuotaResetActivityAborted

Recovery:

1. No action required.

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

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
QuotaResetActivityPaused

Recovery:

1. No action required.

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:

1. No action required.

13160 - xgSDM Ud Sh Create Failed

Alarm Type:
UDR

Description:
This event is generated each time an attempt is made to create a Ud-created subscriber using the Sh interface and it fails.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdShCreateFailed

Recovery:

1. You can contact Customer Support if you want assistance with analysis of the issue.

13161 - xgSDM Ud Bind Request Timeout

Alarm Type:
UDR

Description:
This event in generated each time no response is received within the expected time period for a bind request on an LDAP connection.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdBindRequestTimeout

Recovery:

1. Verify the LDAP connection details configured on the **Main Menu** > **UDR** > **Configuration** > **Ud Client** > **Ud Remote Server Configuration** GUI page are correct on the Ud server.
2. Also verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified LDAP host/port. Check:
   - Host/port details for each primary, secondary, and tertiary connection
   - LDAP bind type (Anonymous, Unauthenticated, or Authenticated)
   - LDAP bind credentials used in the bind request:
     – LDAP authentication DN
     – LDAP authentication password
3. Verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified LDAP host/port.

13162 - xgSDM Ud Bind Request Failed

Alarm Type:
UDR

Description:
This event in generated each time a bind response is received on an LDAP connection which indicates a general failure.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdBindRequestTimeout

Recovery:

1. Verify that the Ud client is attempting to connect to an active Ud server.
2. Verify that the LDAP connection details configured on the **Main Menu** > **UDR** > **Configuration** > **Ud Client** > **Ud Remote Server Configuration** GUI page are correct.
3. Also verify the connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified LDAP host/port. Check:
   - Host/port details for each primary, secondary, and tertiary connection
   - LDAP bind type (Anonymous, Unauthenticated, or Authenticated)
   - LDAP bind credentials used in the bind request:
     – LDAP authentication DN
     – LDAP authentication password
4. Verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified LDAP host/port.

13163 - xgSDM Ud Bind Request Authentication Failed

Alarm Type:
UDR

Description:
This event in generated each time a Bind response is received on an LDAP connection which indicates an authentication failure..

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdBindRequestAuthenticationFailed

Recovery:

1. Verify the LDAP authentication details configured on the **Main Menu** > **UDR** > **Configuration** > **Ud Client** > **Ud Remote Server Configuration** GUI page are correct:
   - The LDAP bind type (Anonymous, Unauthenticated, or Authenticated)
   - The LDAP bind credentials used in the bind request :
     – LDAP authentication DN
     – LDAP authentication password.

13164 - xgSDM Ud Search Request Failed

Alarm Type:
UDR

Description:
This event in generated each time a Search response is received on an LDAP connection which indicates a general failure.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdSearchRequestFailed

Recovery:

1. Check the LDAP error received. Check Ud Server to investigate why error is being returned.

13165 - xgSDM Ud Search Request Authentication Failed

Alarm Type:
UDR

Description:
This event in generated each time a search response is received on an LDAP connection which indicates an authentication failure.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdSearchRequestAuthenticationFailed

Recovery:

1. Check Ud server to determine why error is being returned. Check permissions in LDAP database to ensure that the search request is allowed.

13166 - xgSDM Ud Search Request Unknown Subscriber

Alarm Type:
UDR

Description:
This event in generated each time a search response is received on an LDAP connection which indicates that the subscriber does not exist in the Ud Server.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdSearchRequestUnknownSubscriber

Recovery:

1. Verify that the subscriber exists on the Ud server.
2. Check that SOAP notify requests being sent and processed by the Ud client: check notifications to verify subscriber delete requests on the Ud server are being processed.

13167 - xgSDM Ud Subscribe Request Unknown Subscriber

Alarm Type:
UDR

Description:
This event in generated each time a subscribe response is received on a SOAP connection which indicates that the subscriber does not exist on the Ud server.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdSubscribeRequestUnknownSubscriber

Recovery:

1. Verify that the subscriber exists on the Ud server.
2. Check that SOAP notify requests are being sent and processed by the Ud client: check notifications to verify subscriber delete requests on the Ud server are being processed.

13168 - xgSDM Ud Subscribe Request Failed

Alarm Type:
UDR

Description:
This event in generated each time a subscribe response is received on a SOAP connection which indicates an authentication failure.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdSubscribeRequestFailed

Recovery:

1. Check the HTTP error received.
2. Check Ud server to investigate why error is being returned.

13169 - xgSDM Ud Notify Request Invalid Key

Alarm Type:
UDR

Description:
This event is generated each time an attempt is made to create a Ud-created subscriber using the Sh interface and it fails.

Severity:
Info

Instance:
Connection ID

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdNotifyRequestInvalidKey

Recovery:

1. Verify the key configuration details configured on the **Main Menu** > **UDR** > **Configuration** > **Ud Client Key Details** GUI screen are correct and are as set by the Ud server:
   - Type
   - Ud Attribute
   - Search DN
   - Filter
2. Check that the DN/objectClass sent in the SOAP notify matches the configuration and is the same format as used by the Ud client to send a SOAP subscribe request or an LDAP search request.

13170 - xgSDM Ud Created Subscriber Audit Complete

Alarm Type:
UDR

Description:
This event is generated each time a Ud-created subscriber audit completes. Statistics for each pass are given and are reset for each pass of the audit.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
xgSDMUdCreatedSubscriberAuditComplete

Recovery:

1. 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. It is recommended to contact My Oracle Support for assistance if needed.

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:

1. It is recommended to contact My Oracle Support for assistance if needed.

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:

1. It is recommended to contact My Oracle Support for assistance if needed.

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, it is recommended to contact My Oracle Support for assistance if needed.

13256 - Notification Table Utilization

Alarm Type:
UDR

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

- The rate at which notifications are being produced exceeds the rate at which they can be delivered.
- The servers are unavailable, and the notifications are being buffered for delivery at a later time.

> **Note:** If the number of notifications exceeds the percentage value set for the Major threshold, the notifications received after the threshold is met are cleared. Measurements are pegged.

The alarm severity depends upon the percentage 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:
xgSDMNotificationTableUtilization

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. Check the PCRF to ensure the route is there for the **PCRF MPE** to talk to the User Data Repository message processor.
3. Verify that the application servers are available by checking the **Main Menu** > **UDR** > **Maintenance** > **Subscribing Client Status** page.
4. Depending on the reason that notifications cannot be delivered, it may be necessary to increase the number of notifications that can be stored by User Data Repository. It is recommended to call My Oracle Support.

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:

1. 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:

1. 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.

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.

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.

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.

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.

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.

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.

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, it is recommended to call My Oracle Support.

13362 - Pool Audit Complete

Alarm Type:
UDR

Description:
This event is generated when the last record in the pool audit table is audited. The pool audit report is generated and appears on the View History Report (accessed from the **Alarms & Events** > **View History** GUI page) as part of the text for event 13362. Information included in the report: records visited, total enterprise pools, total subscribers in enterprise pools, and pool audit pass duration (sec).

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
xgSDMAuditStatisticsReportPool

Recovery:

1. No action required.

13363 - User Data Exceeds Max Size

Alarm Type:
UDR

Description:
This event is generated when user data received or sent in a Diameter Sh message exceeds the maximum supported size.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
xgSDMUserDataExceedsMaxSize

Recovery:

1. No action required.

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. It is recommended to call My Oracle Support.

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:

1. Manually start the audit/clean process from **UDR** > **Maintenance** > **Database Auditor**.

13369 - Ud No LDAP Connection

Alarm Type:
UDR

Description:
The Ud client has attempted to open LDAP connections to the Ud server but no LDAP connections can be established after trying primary, secondary (if configured), and tertiary (if configured) connections. This alarm clears when:

1. the Ud client establishes at least one LDAP connection to the Ud server.
2. the Ud client LDAP connections are disabled by configuration.
3. the Ud client LDAP connections are disabled from the **Main Menu** > **UDR** > **Maintenance** > **Ud Client** > **Ud Client Connection Status** GUI page .
4. the Ud client feature is disabled.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
UdNoLDAPConnection

Recovery:

1. Verify the LDAP connection details configured on the **Main Menu** > **UDR** > **Configuration** > **Ud Client** > **Ud Remote Server Configuration** GUI page are correct on the Ud server.
2. Also verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified LDAP host/port. Check:
   - Host/port details for each primary, secondary, and tertiary connection
   - LDAP bind type (Anonymous, Unauthenticated, or Authenticated)
   - LDAP bind credentials used in the bind request:
     – LDAP authentication DN
     – LDAP authentication password
3. Verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified LDAP host/port.

13370 - Ud No SOAP Connection

Alarm Type:
UDR

Description:
The Ud client has attempted to open SOAP connections to the Ud server but no SOAP connections can be established after trying primary, secondary (if configured), and tertiary (if configured) connections. This alarm clears when:

1. the Ud client establishes at least one SOAP connection to the Ud server.
2. the Ud client SOAP connections are disabled by configuration.
3. the Ud client SOAP connections are disabled from the **Main Menu** > **UDR** > **Maintenance** > **Ud Client** > **Ud Client Connection Status** GUI page .
4. the Ud client feature is disabled.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
UdNoSOAPConnection

Recovery:

1. Verify the SOAP connection details configured on the **Main Menu** > **UDR** > **Configuration** > **Ud Client** > **Ud Remote Server Configuration** GUI page are correct on the Ud server.
2. Also verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified SOAP host/port. Check host/port details for each primary, secondary, and tertiary connection.
3. Verify connectivity from the NO servers the host/port details specified; ensure a TCP/IP connection can be established from each NO to each specified SOAP host/port.

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.

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.

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.

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.

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.

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.

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:
MajorMajor (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.

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, it is recommended to call My Oracle Support.

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.

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.

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.

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.

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:

1. 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:

1. 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.

13460 - Client Not Subscribed

Alarm Type:
UDR

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.

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.

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:

1. 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:

1. 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:

1. No action required.

19400-19499 - Transport Manager Alarms and Events

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

19420 - BDFQFull

Alarm Group
SMS

Description
The BDF work queue depth size has reached full capacity.

Severity
Minor

Instance
N/A

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
cAFBDFQFullNotify

Recovery:

1. The system itself may be heavily loaded with work, causing this subsystem to also become overloaded. Check other system resources for signs of overload. It is recommended to contact My Oracle Support for assistance if needed.

19421 - BDFThrotl

Alarm Group
SMS

Description
The BDF subsystem is throttling traffic at sender.

Severity
Minor

Instance
N/A

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
cAFBDFThrotlNotify

Recovery:

1. It is recommended to contact My Oracle Support for assistance if needed.

19422 - BDFInvalidPkt

Alarm Group
SMS

Description
The BDF subsystem received a StackEvent that was somehow invalid, corrupt, or could not be delivered to the application.

Severity
Info

Instance
<Source IP>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
cAFBroadcastDataFrameworkInvalidStackEventNotify

Recovery:

1. If more messages of the same type occur, then check the site(s) and network for other possible corruption or overloaded conditions. It is recommended to contact My Oracle Support for assistance if needed.

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 server, and this may indicate applications on the local server are unable to communicate with all of their peers. Generally this alarm is generated 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. Navigate to **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 by navigating to **Main Menu** > **Alarms & Events** > **View History** for additional **Communication Agent** events or alarms from this **MP** server.

3. Navigate to **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 the remote server is not under maintenance.

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

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

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

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

10. It is recommended to contact My Oracle Support 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

Note: 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.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFConnLocalBlockedNotify

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 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. It is recommended to contact My Oracle Support 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

Note: 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.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFConnRemoteBlockedNotify

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 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. It is recommended to contact My Oracle Support 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. Navigate to **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. It is recommended to contact My Oracle Support for assistance.

2. Navigate to **Status & Manage** > **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.

   It is recommended to contact My Oracle Support 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.

   It is recommended to contact My Oracle Support 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

Note: 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

HA Score:
Normal

Auto Clear Seconds:
300 (5 min)

OID:
cAFClientConnWaitNotify

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.

   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

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. It is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support for assistance.

19806 - Communication Agent CommMessage Mempool Utilization

Alarm Group:
CAF

Description:
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** allocates 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. Navigate to **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. It is recommended to contact My Oracle Support for assistance.

2. Navigate to **Status & Manage** > **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.

   It is recommended to contact My Oracle Support 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 ingres rate to the server site is exceeding its capacity.

   It is recommended to contact My Oracle Support 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. Navigate to **Alarms & Events** to examine the alarm log and determine if the ComAgent worker thread may be experiencing a problem preventing it from processing events from User Data FIFO queue.

2. Navigate to **Status & Manage** > **KPIs** to monitor the ingress traffic rate of each MP.
   - Mis-configuration of routing may result in unbalanced traffic directed to the MP. Under balanced traffic distribution, each MP 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 offered load to the server site is exceeding its capacity.
3. There may be an issue with network that causes lot of ComAgent connection setup and handshake messages. Check network latency and stability parameters.
4. If the problem persists, it is recommended to contact My Oracle Support 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. 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.

   It is recommended to contact My Oracle Support for assistance.
2. An IP network or adjacent node problem may exist preventing transmission of messages into the network at the same pace the messages are being received from the network.
3. Navigate to **Status & Manage** > **KPIs** to monitor the ingress traffic rate of each MP.

- The mis-configuration of adjacent node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
- 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.

4. If the problem persists, it is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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.

> **Note:** 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.

Severity:
Info

Instance:
N/A

HA Score:
Normal

OID:
cAFEventComAgtConfigParamChangeNotify

Recovery:

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**. It is recommended to contact My Oracle Support 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:

1. If the problem persists, it is recommended to contact My Oracle Support.

19820 - Communication Agent Routed Service Unavailable

Alarm Group:
CAF

Description:
This alarm indicates 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. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the reasons why connections are unavailable.
3. Navigate to **Main Menu** > **Status & Manage** > **Server** to confirm the far-end servers have an application state of enabled, and their subsystems are operating normally.

   This alarm can result from conditions at the far-end servers connected to the server that asserted this alarm.

4. Check network and reach-ability of provider server(s) from user server(s). Loss of network connectivity can lead to this alarm. In that case, the user also sees alarm 19800.
5. It is recommended to contact My Oracle Support 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 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. It is recommended to contact My Oracle Support for assistance.

19822 - Communication Agent Routed Service Congested

Alarm Group:
CAF

Description:
This alarm indicates 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. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the are congested and the degree to which they are congested.
3. Check the far-end of the congested connections to further isolate the cause of congestion.

   If the far-end servers are overloaded, then it is possible 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. It is recommended to contact My Oracle Support 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.
4. It is recommended to contact My Oracle Support for assistance.

19824 - Communication Agent Pending Transaction Utilization

Alarm Group:
CAF

Description:
The **ComAgent** Reliable Transfer Function is approaching or exceeding its engineered reliable transaction handling capacity.

Severity:
Minor, Major, Critical

Instance:
N/A (ComAgent process)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFTransUtilNotify

Recovery:

1. Navigate to **Status & Manage** > **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 **Alarm & Events** to examine the alarm log.

   The system may be experiencing network problems.

   The **Communication Agent** Process may be experiencing problems.
5. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19825 - Communication Agent Transaction Failure Rate

Alarm Group:
CAF

Description:
The number of failed transactions during the sampling period has exceeded configured thresholds.

Severity:
Minor, Major, Critical

Instance:
<ServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFTransFailRateNotify

Recovery:

1. Navigate to **Status & Manage** > **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. Navigate to **Alarm & Events** to examine the alarm log.

   The system may be experiencing network problems.

   The **Communication Agent** process may be experiencing problems.
5. It is recommended to contact My Oracle Support for assistance.

19826 - Communication Agent Connection Congested

Alarm Group:
CAF

Description:
This alarm indicates **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. Navigate to **Alarms & Events** > **View History** to find additional information for the alarm by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Navigate to **Alarms & Events** > **View History** to check the event history logs for additional Communication Agent events or alarms from this MP server.
3. Navigate to **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 the remote server is not under maintenance.
   b. Examine the remote's CPU utilization.
5. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19827 - SMS stack event queue utilization

Alarm Group:
SMS

Description:
The percent utilization of the SMS Task stack queue is approaching defined threshold capacity.

Severity:
Minor, Major, Critical

Instance:
<SMS Thread/Queue Index>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFSmsQueueUtilNotify

Recovery:

1. The system itself may be heavily loaded with work, causing this subsystem to also become overloaded. Check other system resources (ComAgent Congestion, Cpu Utilization, and Server Congestion are some examples) for signs of overload.
2. If the problem persists, it is recommended to contact My Oracle Support 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:

1. This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.

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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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:

1. 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:

1. 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:

1. 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:

1. 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. It is recommended to contact My Oracle Support 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:

1. Navigate to **Communication Agent** > **Maintenance** > **Connection Status** to verify 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, navigate to **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 maintenance actions have removed the application from service that provides the concerned resource.

3. It is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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:

1. 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:

1. 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:

1. 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. It is recommended to contact My Oracle Support 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:

1. 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. It is recommended to contact My Oracle Support 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:

1. 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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support 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/Gen9 hardware, 75k on other hardware
- Major - if exceeding 110K on Gen8/Gen9 hardware, 80k on other hardware
- Critical - if exceeding 120K on Gen8/Gen9 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. It is recommended to contact My Oracle Support 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. It is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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:

1. 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:

1. 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. It is recommended to contact My Oracle Support 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. Navigate to **Status & Manage** > **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. Navigate to **Alarms & Events** to examine the alarm log.

It is recommended to contact My Oracle Support 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:

1. An unexpected condition has occurred while performing a database update, but database updates are still enabled.

   It is recommended to contact My Oracle Support 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:

1. An unexpected condition has occurred while performing a database update and database updates are disabled.

   It is recommended to contact My Oracle Support 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:

1. An unexpected condition has occurred while performing a database update, but database updates are still enabled.

   It is recommended to contact My Oracle Support 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:

1. An unexpected condition has occurred while performing a database update and database updates are disabled.

   It is recommended to contact My Oracle Support 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:

1. Measurement subsystem initialization has failed for the specified measurement.

   It is recommended to contact My Oracle Support for assistance.

22000-22999 - Diameter

This section provides information and recovery procedures for Diameter alarms and events, 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>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterIngressMsgRejectedDecodingFailureNotify

Recovery:

1. During Diameter Request decoding, the message content was inconsistent with the "Message Length" in the message header. This protocol violation can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

22002 - Peer Routing Rules with Same Priority

Event Type:
DIAM

Description:
A peer routing table search with a received Request message found more than one highest priority Peer Routing Rule match. The system selected the first rule found but it is not guaranteed that the same rule will be selected in the future. It is recommended that Peer Routing Rules be unique for the same type of messages to avoid non-deterministic routing results.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterPeerRoutingTableRulesSamePriorityNotify

Recovery:

1. Modify one of the Peer Routing Rule Priorities using the **Diameter > Configuration > Peer Routing Rules** GUI page.

22003 - Application ID Mismatch with Peer

Event Type:
DIAM

Description:
While attempting to route a request message to a peer, a peer's transport connection was bypassed because the peer did not support the Application ID for that transport connection.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterApplicationIdMismatchWithPeerNotify

Recovery:

1. The system's peer routing table may be using a Route List containing a peer which does not support the Application ID or the list of Application IDs supported by the peer on each connection may not be the same. The list of Application IDs that the peer supports on each connection can be viewed as follows:
   a. Navigate to the GUI page: **Diameter > Maintenance > Connections**
   b. Locate the relevant Peer Node and check the supported Application IDs.
2. If Application IDs are not the same for each connection (but should be) the Application ID for any connection can be refreshed by:
   a. Navigate to the GUI page: **Diameter > Maintenance > Connections**
   b. Locate the relevant **Connection**
   c. Disable the **Connection**
   d. Enable the **Connection**
3. The Diameter Node which originated the message (identified by the Origin-Host AVP) could be configured incorrectly and the application is trying to address a

node which doesn't support the Application ID. This cannot be fixed using this application.

4. If the problem persists, contact My Oracle Support.

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:

1. 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. It is recommended to contact My Oracle Support 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. View and update the Peer Routing Rules by navigating to **Diameter > Configuration > Peer Routing Rules**.
2. If multiple peer routing tables are used, ensure the correct table is applied for the message in question.
3. If the problem persists, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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:

1. If this event is occurring frequently, the transaction timers may be set too low. Navigate to **Diameter > Configuration > Pending Answer Timers** to view and/or modify the Pending Answer Timer, Transaction Request Lifetime, peer node settings.

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support 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:

1. It is recommended to contact My Oracle Support 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.

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 and it exceeds the configurable alarm threshold.

> **Note:** The alarm thresholds are configurable using the Alarm Threshold Options tab on **Diameter** > **Configuration** > **System Options**.

When this alarm is generated, the system clears all individual peer node alarms (alarm 22051) for the peer node. These alarms can be viewed in **Alarms & Events** > **View Active**.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPeerNodeUnavailableThresholdReachedNotify

Recovery:

1. Navigate to **Diameter** > **Maintenance** > **Peer Nodes** to monitor peer status.

2. Verify IP network connectivity exists between the MP server and the peer node.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify the peer is not under maintenance.
5. It is recommended to contact My Oracle Support 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 **Diameter** > **Configuration** > **System Options**.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRouteListUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Route Lists** to monitor Route List status.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List are not under maintenance.
5. It is recommended to contact My Oracle Support 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:

1. 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:

1. 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

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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support.

22022 - Forwarding Loop Detected

Alarm Group:
DIAM

Description:
Ingress Request message received was previously processed by the local node as determined from the Route-Record AVPs received in the message.

Severity:
Major

Instance:
<Peer Name>

HA Score:
Normal

Auto Clear Seconds:
30

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 mis-routing the message. This should not be related to a configuration error because the identity of the local node is sent to the peer during the Diameter Capabilities Exchange procedure when the Connection comes into service.
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, it is recommended to contact My Oracle Support.

22051 - Peer Unavailable

Alarm Group:
DIAM

Description:
Unable to access the Diameter Peer because all of the transport connections are down. Peer node unavailability can happen in these cases:

- All connections toward a peer are no longer candidates for routing Request messages.
- No available connections within the peer node support the Application ID. This is functionally equivalent to the peer node being unavailable.
- The Connection Priority Level (CPL) value for a resource is changed to 99, which means the operational status is Unavailable. The CPL value of a connection can be found in the active SO under **Diameter** > **Maintenance** > **Connections**.
- The number of established connections drops below the configured Minimum Connection Capacity.

Severity:
Critical

Instance:
<PeerName> (of the Peer which failed).

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPeerUnavailableNotify

Recovery:

1. Confirm a connection is provisioned for the peer node.
    - Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
    - Verify IP network connectivity exists between the MP server and the peer nodes using ping, traceroute, or other means.
    - Examine the event history logs for additional DIAM events or alarms from the MP server.
    - Verify the peer is not under maintenance.
    - Verify there are connections provisioned for the peer node.
    - Verify the status of all connections toward the peer node.

      From the active SO GUI, navigate to **Diameter** > **Maintenance** > **Peer Nodes**. View the Transaction Configuration Set of the peer node.

      If the peer node has a corresponding Transaction Configuration Set setting, then navigate to **Diameter** > **Configuration** > **Configuration Sets** > **Transaction Configuration Sets** and confirm the Application ID is supported.

2. Confirm the peer node supports the Application ID in the request message.
3. Resolve any congestion issues on the peer node.
4. If the problem persists, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

22053 - Route List Unavailable

Alarm Group:
DIAM

Description:
All route groups with the route list are 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 periodically attempts to recover the connection automatically if its Admin State is

enabled. If the Transport Connection is configured for Responder-Only mode, the peer is responsible for re-establishing the transport connection.

Examine the Event history and software release information for the route groups.

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 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 the peers in the route list not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support.

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 periodically attempts to recover the connection if its admin state is enabled. If the transport connection is configured for responder-only mode, the peer is 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. Verify Route List status and configured minimum capacity from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify 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 the peers in the Route List are not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

22057 - ETG Rate Limit Degraded

Alarm Group:
DIAM

Description:
The **ETG** Rate Limit has exceeded the defined threshold.

Severity:
Major

Instance:
<ETGName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgRateLimitDegradedNotify

Recovery:

1. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.

2. Check the Egress Message Rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Main Menu** > **Diameter** > **Maintenance** > **Connections** to determine if the sending Peers/Connections are offering too much traffic.

3. If the problem persists, it is recommended to contact My Oracle Support.

22058 - ETG Pending Transaction Limit Degraded

Alarm Group:
DIAM

Description:
The **ETG** Pending Transactions Limit has exceeded the defined threshold.

Severity:
Major

Instance:
<ETGName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgPendingTransLimitDegradedNotify

Recovery:

1. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Main Menu** > **Diameter** > **Maintenance** > **Connections** to determine if the sending Peers/Connections are offering too much traffic.
3. Determine if the receiving Peers or Connections in the **ETG** are not responding with Answers in a timely manner because they are either busy or overloaded.
4. If the problem persists, it is recommended to contact My Oracle Support.

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 an **ETG**. However, if that is not the case, alternate routes may be out of service and could cause overloading of traffic towards connections contained in this **ETG**. Evaluate traffic distribution to server connections and see if any alternate routes to server are unavailable causing overloading of traffic on an **ETG**.
4. It is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support.

22062 - Actual Host Name cannot be determined for Topology Hiding

Event Group:
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, it is recommended to contact My Oracle Support.

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:

1. No action required. However, if this event is seen to be incrementing consistently, it is recommended to contact My Oracle Support 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, it is recommended to contact My Oracle Support

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, it is recommended to contact My Oracle Support

22066 - ETG-ETL Scope Inconsistency

Alarm Group:
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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

22068 - TtpEvDoicException

22068 - 001 - TtpEvDoicException: DOIC OC-Supported-Features AVP not received

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:001

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. The Peer Node associated with the TTP is not responding to a DOIC Capability Announcement (DCA). This can occur when the Peer Node either does not support DOIC or DOIC has been disabled on the Peer Node. The operator should either disable DOIC on the DSR associated with TTP by setting the TTP's "Dynamic Throttling Admin State" to Disabled or enable DOIC on the Peer Node.

22068 - 002 - TtpEvDoicException: DOIC OC-Feature-Vector AVP contains an invalid value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:002

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. The Peer Node associated with the TTP has selected a DOIC Abatement Algorithm not supported by the TTP. This should never happen and may be the result of a mis-configuration or bug on the Peer Node. If this error persists, the operator should disable DOIC for the TTP by setting the TTP's "Dynamic Throttling Admin State" to Disabled or enable DOIC on the Peer Node.

22068 - 003 - TtpEvDoicException: DOIC OC-Report-Type AVP contains an unsupported value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:003

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. The Peer Node associated with the TTP is sending a DOIC overload report which is not supported by DSR at this time. The operator should disable Realm-based DOIC overload reports on the Peer Node.

22068 - 004 - TtpEvDoicException: DOIC OC-Sequence-Number AVP contains an out of order sequence number

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:004

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. The Peer Node associated with the TTP has sent a DOIC overload report that is out of sequence. If this error occurs infrequently, then it may have been caused by a timing delay whereby Answer messages received from the Peer Node were delivered out of order. If this error occurs frequently, then the Peer Node may be in violation of the DOIC specification.

22068 - 005 - TtpEvDoicException: DOIC OC-Reduction-Percentage AVP contains an invalid value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:005

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. The Peer Node associated with the TTP has sent a DOIC overload report containing an OC-Reduction-Percentage AVP value greater than 100. If this error occurs

infrequently, then there may be a DOIC software error in the Peer Node. If this error occurs frequently, then the error may be caused by a Peer Node DOIC mis-configuration problem.

22068 - 006 - TtpEvDoicException: DOIC OC-Validity-Duration AVP contains an invalid value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:006

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. The Peer Node associated with the TTP has sent a DOIC overload report containing an OC-Validity-Duration AVP value greater than the maximum allowed. The maximum value for the OC-Validity-Duration AVP is 86,400 seconds (24 hours). If this error occurs infrequently, then there may be a DOIC software error in the Peer Node. If this error occurs frequently, then the error may be caused by a Peer Node DOIC mis-configuration problem.

22069 - 001 - TtpEvDoicOlr: Valid DOIC OLR Applied to TTP

Event Type:
DIAM

Description:
A DOIC OverLoad Request (OLR) was received from a Peer Node and applied to a configured TTP.

Severity:
Info

Instance:
<TTP Name>:001

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. No action required.

22070 - TtpEvDegraded

22070 - 001 - TtpEvDegraded: TTP Degraded, Peer Overload

Event Type:
DIAM

Description:
TTP Degraded

Severity:
Info

Instance:
<TTP Name>:001

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDegradedNotify

Recovery:

1. No action required.

22070 - 002 - TtpEvDegraded: TTP Degraded, Peer Overload Recovery

Event Type:
DIAM

Description:
TTP Degraded

Severity:
Info

Instance:
<TTP Name>:002

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDegradedNotify

Recovery:

1. No action required.

22070 - 003 - TtpEvDegraded: TTP Degraded, Static Rate Limit Exceeded

Event Type:
DIAM

Description:
TTP Degraded

Severity:
Info

Instance:
<TTP Name>:003

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDegradedNotify

Recovery:

1. No action required.

22071 - 001 - TtgEvLossChg: TTG Loss Percent Changed

Event Type:
DIAM

Description:
TTG's Loss Percentage was modified.

Severity:
Info

Instance:
<TTG Name>:001

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

Recovery:

1. No action required.

22072 - TTP Degraded

Alarm Group
DIAM

Description
The TTP's Operational Status has been changed to Degraded.

Severity
Major

Instance
<TTP Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtpDegradedNotify

Recovery

1. No action required.

22073 - TTP Throttling Stopped

Alarm Group
DIAM

Description
TTP rate throttling has been suspended due to an internal failure.

Severity
Minor

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtpThrottlingStoppedNotify

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, it is recommended to contact My Oracle Support.

22074 - TTP Maximum Loss Percentage Threshold Exceeded

Alarm Group
DIAM

Description
The Maximum Loss Percentage Threshold assigned to the TTP has been exceeded.

Severity
Major

Instance
<TTP Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtpMaxLossPercentageExceededNotify

Recovery

1. No action required.

22075 - Message is not routed to Application

Alarm Group:
DIAM

Description:
ART Rule-X was selected, but message was not routed because DSR Application is disabled or not available.

Severity:
Major

Instance:
<DSR Application Name>

HA Score:
Normal

Auto Clear Seconds:
0

OID:
eagleXgDiameterArtMatchAppUnavailableNotify

Recovery:

1. Check the Application Status by navigating to **Diameter** > **Maintenance** > **Applications** and Enable the application if the Admin State of the DSR application is Disabled for a particular DA-MP(s) which raised the alarm.
2. If the Application is Enabled for a particular DA-MP, but the Operational Status is Unavailable or Degraded, then refer to the Operational Reason and rectify it accordingly.
3. If the problem persists, it is recommended to contact My Oracle Support.

22076 - TTG Maximum Loss Percentage Threshold Exceeded

Alarm Group
DIAM

Description
The "Maximum Loss Percentage Threshold" assigned to the Route Group within the Route List has been exceeded.

Severity
Major

Instance
<Route List Name>:<Route Group Name>.<TTG Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtgMaxLossPercentageExceededNotify

Recovery

1. No action required.

22077 - Excessive Request Reroute Threshold Exceeded

Alarm Group:
DIAM

Description:
Request reroutes due to Answer response and/or Answer timeout having exceeded the configured onset threshold percentage on the DA-MP server.

Severity:
Major

Instance:
MpReroutePercent

HA Score:
Normal

Auto Clear Seconds:
N/A

> **Note:** The alarm clears when the percentage of Request reroutes due to Answer Result-code matching "Reroute on Answer" and Answer Timeout drops below the configured abatement threshold and remains there for the configured abatement time. The alarm also clears when the DSR process is stopped or restarted.

OID:
eagleXgDiameterMpExcessiveRequestRerouteNotify

Recovery:

1. This alarm is an indication of reroutes exceeding the configured threshold, due to responses from the Peer Node exceeding the Pending Answer timer in DSR or due to configured "Reroute on Answer" Result codes.
2. If rerouting is triggered due to Answer Result-code:
   a. Use measurement TxRerouteAnswerResponse to identify any peer (or set of peers) being identified as triggering reroute.
   b. If a peer (or set of peers) is identified, validate that Reroute-on-Answer is properly configured for that peer.
   c. Check for congestion being reported by the peer (**Diameter** > **Maintenance** > **Peer Node**).
3. If rerouting is triggered due to Answer Timeout:
   a. Use measurement TxRerouteAnswerTimeout to identify any peer (or set of peers) being identified as timing out.
   b. If a peer (or set of peers) is identified, verify that Pending Answer Timer and Transaction Lifetime are properly configured.
   c. Check for congestion being reported by the peer (**Diameter** > **Maintenance** > **Peer Node**).
4. If the problem persists, it is recommended to contact My Oracle Support.

22078 - Loop or Maximum Depth Exceeded in ART or PRT Search

Alarm Group:
DIAM

Description:
An ART/PRT search has resulted in either a loop between ART/PRT tables, or the search depth has exceeded the maximum allowed depth.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterNestedArtPrtSearchErrorNotify

Recovery:

1. If the error was a search loop, the customer should change at least one of the rules in the search sequence to avoid a loop. If the error was a maximum depth exceeded, the customer should remove one or more rules in the search sequence.
2. If the problem persists, it is recommended to contact My Oracle Support.

22101 - Connection Unavailable

Alarm Group:
DIAM

Description:
Connection is unavailable for Diameter Request/Answer exchange with peer.

> **Note:** This alarm is not raised when the Suppress Connection Unavailable alarm for a Transport Connection is set to Yes.

Alarm 22101 is generated when the connection's administrative state is enabled and the connection is not in a state where it can send or receive Diameter Requests or Answers to/from the peer. The alarm is generated when one of the following occurs.

- Connection's Admin State transitions from disabled to enabled
- Connection's Operational Status transitions from available to unavailable
- Connection's Operational Status transitions from degraded to unavailable

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnectionUnavailableAlarmNotify

Recovery:

1. Confirm the host IP interface is down or unreachable from the peer.
2. Confirm the peer IP interface is down or unreachable from the host.
3. Verify the following are configured and available:
   - Remote IP availability
   - Remote server (port) availability
   - Network availability
   - Local IP route to remove
   - Local MP service availability
   - Configuration correctness, such as CEX parameter matching with remove
4. 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.
5. If the problem persists, it is recommended to contact My Oracle Support.

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. This alarm is generated when:

- Connection congestion when the DSR Tx sender buffer is at maximum capacity
- The connection's administrative state is enabled and the connection is in congestion. Requests and Answers continue to be received and processed from the peer over the connection, and attempts to send Answers to the peer still occur. The alarm is raised when one of the following occurs:

  - Connection's Operational Status transitions from available to degraded (connection has become congested or watchdog algorithm has failed)
  - Connection's Operational Status transitions from unavailable to degraded (connection has successfully completed the capabilities exchange and is performing connection proving)
- Connection egress message rate threshold has been crossed
- Diameter connection is in watchdog proving
- Diameter connection is in graceful disconnect
- Diameter peer signaled the remote is busy
- Diameter connection is in transport congestion

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterFsmOpStateDegraded

Recovery:

1. View the Connection Performance measurement report for the +/- 1 hour congestion event.
2. Examine the log file by using these commands:
   - `# date >> tcp_stat_<hostname>`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# date >> tcp_stat_<hostname>`
3. Examine the output of the command `netstat -canp --tcp | grep <remote IP:Port for conn>` for few minutes.

4. Examine the corresponding Rx buffer on the connection in question using this command:`netstat -canp --tcp | grep <remote IP:Port for conn>`. The RxBuffer value is configured using ConnectionCfget.
5. Examine the overall network statistics for other issues using the command `netstat -i`.
6. Examine the overall network delay using the command `ping`.
7. View the software release information.
8. 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.
9. Have the peer vendor examined their receive buffer usage during the event; if it is 0, this means the received messages were processed quickly and messages were not often stored in the receive buffer. In this case, Egress Transport Congestion was due to the peer not processing the message quickly enough (verify by examining the peer's receive buffer), or there is some delay introduced in the network
10. If the problem persists, it is recommended to contact My Oracle Support.

22103 - SCTP Connection Impaired

Alarm Group:
DIAM

Description:
One or more paths of the SCTP multi-homed connection is down.

Severity:
Minor

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterSCTPConnectionImpairedAlarmNotify

Recovery:

1. The alarm clears when the connection is operationally unavailable or all paths are operationally available.

   Potential causes are:

   - A host IP interface is down.
   - A host IP interface is unreachable from the peer.
   - A peer IP interface is down.

- A peer IP interface is unreachable from the host.
- Network path is down between one host IP and the other peer IP.
- Network congestion or large latency in network (resulting loss or late arrival of packets).

2. 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.
3. If the problem persists, it is recommended to contact My Oracle Support.

22104 - SCTP Peer is Operating with a Reduced IP Address Set

Alarm Group:
DIAM

Description:
The SCTP peer advertised less IP addresses than configured for the connection. If two IP addresses have been configured for the Local Node of a certain SCTP connection, but following the SCTP connection establishment the peer node has advertised only one IP address (less than the number of IP addresses configured for the local node), then Alarm 22104 is generated.

Severity:
Minor

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterSCTPPeerReducedIPSetAlarmNotify

Recovery:

1. When the operational status is Available and a connection is established over SCTP transport, the number of IP addresses advertised by the peer in INIT/INIT_ACK is less than the number of paths set by the connection configuration. For instance, the established connection has two IP addresses configured for the Local Node, but the peer node has advertised only one IP address.
2. 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.
3. If the problem persists, it is recommended to contact My Oracle Support.

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.

22200 - MP CPU Congested

Alarm Group:
ExgStack

Description:
DA-MP CPU utilization threshold has been exceeded. Potential causes are:

- One or more peers are generating more traffic than is normally expected
- Configuration requires more CPUs for message processing than is normally expected
- One or more peers are answering slowly, causing a backlog of pending transactions
- A DA-MP has failed, causing the redistribution of traffic to the remaining DA-MPs

Severity:
Minor, Major, Critical, Warning

Instance
NA

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpCpuCongestedNotify

Recovery:

1. If one or more MPs in a server site has failed, the traffic is distributed between the remaining MPs in the server site. Monitor the **MP** server status from **Status & Manage** > **Server**.
2. The mis-configuration of DIAMETER peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each **MP** from **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 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. Examine the alarm log from **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

22201 - MpRxAllRate

Alarm Group:
DIAM

Description:
DA-**MP** ingress message rate threshold crossed.

Severity:
Minor, Major, Critical

Instance:
MpRxAllRate, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpRxAllRateNotify

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, it is recommended to contact My Oracle Support.

22202 - MpDiamMsgPoolCongested

Alarm Group:
DIAM

Description:
DA-**MP** Diameter message pool utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
MpDiamMsgPool, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpDiamMsgPoolCongestedNotify

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

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, it is recommended to contact My Oracle Support.

22207 - DclTxTaskQueueCongested

Alarm Group:
DIAM

Description:
DCL egress task message queue utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<DA-MP Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDclTxTaskQueueCongested

Recovery:

1. The alarm will clear when the DCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

22208 - DclTxConnQueueCongested

Alarm Group:
DIAM

Description:
DCL egress connection message queue utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<ConnectionName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDclTxConnQueueCongested

Recovery:

1. The alarm will clear when the DCL egress connection message queue utilization falls below the clear threshold. The alarm may be caused by peers being routed more traffic than nominally expected.
2. It is recommended to contact My Oracle Support 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.

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, it is recommended to contact My Oracle Support.

22221 - Routing MPS Rate

Alarm Group:
DIAM

Description:
Message processing rate for this **MP** is approaching or exceeding its engineered traffic handling capacity. The routing mps rate (MPS/second) is approaching or exceeding its engineered traffic handling capacity for the MP.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRoutingMpsRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site.

   MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP.

   The routing mps rate of each **MP** can be monitored from **Main Menu** > **Status & Manage** > **KPIs**. Each **MP** in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load.

   The routing mps rate of each **MP** can be monitored from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state then the ingress message rate to the **MP** is exceeding its capacity to process the messages.

4. If the problem persists, it is recommended to contact My Oracle Support.

22222 - Long Timeout PTR Buffer Pool Utilization

Alarm Group:
DIAM

Description:
The MP's Long Timeout PTR buffer pool is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterLongTimeoutPtrBufferPoolUtilNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Pending Answer Timer assignment may result in excessive traffic being assigned to the Long Timeout PTR buffer Pool. View the Pending Answer Timer values via **Diameter** > **Configuration** > **Pending Answer Timers**. Examine the Pending Answer Timers assignment via the **Diameter** > **Configuration** > **Application Ids and Diameter** > **Configuration** > **Peer Nodes**.
3. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second
4. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
5. A software defect may exist resulting in Long Timeout PTR buffers not being de-allocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log from **Main Menu** > **Alarms & Events**.
6. If the problem persists, it is recommended to contact My Oracle Support.

22223 - MpMemCongested

Alarm Group:
DIAM

Description:
DA-**MP** memory utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
System.RAM_UtilPct, DSR

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpMemCongestedNotify

Recovery:

1. Potential causes for this alarm are:

   - One or more peers are generating more traffic than is nominally expected.
   - Configuration requires more CPU usage for message processing than is nominally expected.
   - One or more peers are answering slowly, causing a backlog of pending transactions.

22224 - Average Hold Time Limit Exceeded

Alarm Group:
DIAM

Description:
The average transaction hold time has exceeded its configured limits.

This alarm is generated when KPI #10098 (TmAvgRspTime) exceeds DSR-wide engineering attributes associated with average hold time, defined in the DA-MP profile assigned to the DA- MP server. KPI #10098 is defined as the average time (in milliseconds) from when the routing layer (DRL) receives a request message from a downstream peer to the time that an answer response is sent to that downstream peer. The source measurement of KPI #10098 is the TmResponseTimeDownstreamMp (10093) measurement.

This alarm indicates the average response time (TmAvgRspTime) for messages forwarded by the Relay Agent is larger than what is defined for a deployment as per DA-MP profile assignment. One of these problems could exist:

- The IP network may be experiencing problems that are adding propagation delays to the forwarded request message and the answer response.
  - Verify the IP network connectivity exists between the MP server and the adjacent nodes.
  - View the event history logs for additional events or alarms from this MP server.
- One or more upstream nodes may be experiencing traffic overload.
- One or more MPs is experiencing traffic overload.
  - View the KPI Routing Recv Msgs/Sec.
  - View the CPU utilization of MPs by navigating to **Main Menu** > **Status & Manage** > **Server**.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterAvgHoldTimeLimitExceededNotify

Recovery:

1. The average transaction hold time is exceeding its configured limits, resulting in an abnormally large number of outstanding transactions that may be leading to excessive use of resources like memory.

   - Reduce the average hold time by examining the configured Pending Answer Timer values and reducing any values that are unnecessarily large or small.
   - Identify the causes for the large average delay between the DSR sending requests to the upstream peers and receiving answers for the requests.
   - Confirm the peer node(s) or DSR is in overload by viewing KPI/Measurements/CPU usage and take corrective action.
   - Identify the main contributor to increased value of (T2-T1) such as a time difference between the routing layer (DRL) receiving the request to the DRL sending the answer to downstream peer.

2. The alarm thresholds are configurable on **Diameter Common** > **MPs** > **Profiles**:

   - Average hold time minor alarm onset threshold
   - Average hold time minor alarm abatement threshold
   - Average hold time major alarm onset threshold
   - Average hold time major alarm abatement threshold
   - Average hold time critical alarm onset threshold
   - Average hold time critical alarm abatement threshold

   The severity of the alarm (Minor, Major, or Critical) is according to the onset threshold/abatement threshold of each severity level. When the average hold time initially exceeds the average hold time for an alarm onset threshold, a minor, major, or critical alarm is triggered. When the average hold time subsequently exceeds a higher onset threshold, or drops below an abatement threshold, but is still above the minor alarm abatement threshold, the alarm severity changes based on the highest onset threshold crossed by the current average hold time.

3. If the problem persists, it is recommended to contact My Oracle Support.

22225 - Average Message Size Limit Exceeded

Alarm Group:
DIAM

Description:
The size of the average message processed by DSR has exceeded its configured limits.

The alarm is generated when the measurement RxAvgMsgSize reaches the DSR-wide engineering attributes, defined in the DaMpProfileParameters corresponding to the MP profile being used. RxAvgMsgSize is defined as the size of the average message processed by DSR.

This alarm indicates DSR has encountered a message it can accept for processing, but might not continue processing if the message size increases more than the maximum supported message size. This increase can be due to standard diameter processing (for example, Route Record additions to requests) or due to custom processing (for example, Mediation modifying AVPs).

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterAvgMsgSizeLimitExceededNotify

Recovery:

1. Examine the traffic coming from connected peers to see if any of them are sending abnormally large messages, and look for any special processing rules being applied by DSR to that message.
2. The alarm thresholds are configurable on **Diameter Common** > **MPs** > **Profiles**:
   - Average hold time minor alarm onset threshold
   - Average hold time minor alarm abatement threshold
   - Average hold time major alarm onset threshold
   - Average hold time major alarm abatement threshold
   - Average hold time critical alarm onset threshold
   - Average hold time critical alarm abatement threshold

   The severity of the alarm (Minor, Major, or Critical) is according to the onset threshold/abatement threshold of each severity level. When the average hold time initially exceeds the average hold time for an alarm onset threshold, a minor, major, or critical alarm is triggered. When the average hold time subsequently exceeds a higher onset threshold, or drops below an abatement threshold, but is still above the minor alarm abatement threshold, the alarm severity changes based on the highest onset threshold crossed by the current average hold time.

3. If the problem persists, it is recommended to contact My Oracle Support.

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.

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.

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.

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.

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.

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:
eagleXgDiameterConnUnavailCerHostIpAvpVldtnFailNotify

Recovery:

1. Diagnose peer to resolve inconsistency.
2. If the problem persists, contact My Oracle Support.

22328 - IcRate

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:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterImr

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.

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.

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. It is recommended to contact My Oracle Support for assistance.

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

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterConnRejMHSctpConnAttemptNotify

Recovery:

1. Update the peer to initiate unihomed IPFE SCTP connections.
2. It is recommended to contact My Oracle Support 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.

The Alarm Thresholds are configurable using the Alarm Threshold Options tab on **Diameter** > **Configuration** > **System Options**.

The IPFE connection may not be established for a variety of reasons. The operational status of this connection is displayed on the GUI as unavailable and Alarm 22101 Connection Unavailable is raised.

When the number of unavailable IPFE connections exceeds the defined threshold, IPFE Connection Failure Major/Critical Aggregation Alarm Threshold (default is 100/200), alarm 22349 is raised by the DSR.

Severity:
Major, Critical

> **Note:** The Critical threshold may be disabled by setting the Critical Threshold to zero using the Alarm Threshold Options tab on **Diameter** > **Configuration** > **System Options**.

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIPFEConnUnavailableThresholdReachedNotify

Recovery:

1. Navigate to **Diameter** > **Maintenance** > **Connection** to monitor IPFE Connection status.

2. Confirm peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm 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 the peers in the Route List are not under maintenance.
5. Use Wireshark to analyze all the captured PCAP data to find where the message exchange is broken or failed. Wireshark should be the main tool used to diagnose the unavailable connection.
6. Based on the PCAP file, correct the configuration if the issue is on the DSR side. The Alarm will be cleared automatically when the numbers of unavailable IPFE connections are under the IPFE Connection Failure Critical/Major Aggregation Alarm Threshold.
7. If the issue is on the DSR side or you are not sure, it is recommended to contact My Oracle Support 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 **Diameter** > **Configuration** > **System Options**.

Severity:
Major, Critical

Note: The Critical threshold may be disabled by setting the Critical Threshold to zero using the Alarm Threshold Options tab on **Diameter** > **Configuration** > **System Options**.

Instance:
<DA-MP-Hostname>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnUnavailableThresholdReachedNotify

Recovery:

1. Navigate to **Main Menu** > **Diameter** > **Maintenance** > **Connection** to monitor Fixed Connection status.
2. Confirm the peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm 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 the peers in the Route List are not under maintenance.
5. Navigate to **Diameter** > **Configuration** > **System Options** to check the Alarm Threshold Options setting. Modify the value if it is set too low.
6. It is recommended to contact My Oracle Support for assistance.

22900 - DPI DB Table Monitoring Overrun

Event Type:
DIAM

Description:
The COMCOL update sync log used by DB Table monitoring to synchronize Diameter Connection Status among all DA-MP RT-DBs has overrun. The DA-MP's Diameter Connection Status sharing table is automatically audited and re-synced to correct any inconsistencies.

Severity:
Info

Instance:
<DbTblName>

> **Note:** <DbTblName> refers to the name of the Diameter Connection Status Sharing Table the Diameter Connection status inconsistency that was detected.

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDpiTblMonCbOnLogOverrunNotify

Recovery:

1. It is recommended to contact My Oracle Support 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:

1. It is recommended to contact My Oracle Support.

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:

1. No action necessary.

Note: DA-**MP**'s SLDB tables are automatically audited and re-synchronized to correct inconsistencies after a log overrun has occurred. The Automatic Data Integrity Check, which was introduced in cm6.2, periodically scans almost the entire local IDB for integrity. The initial default period is 30 minutes.

22960 - DA-MP Profile Not Assigned

Alarm Group:
DIAM

Description:
This alarm is generated when a DA-MP is brought into service and a DA-MP configuration profile has not been assigned to the DA-MP during DSR installation/upgrade procedures.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDaMpProfileNotAssignedNotify

Recovery:

1. From the DSR OAM GUI, navigate to **Diameter Common** > **MPs** > **Profile Assignments** to assign a DA-MP profile to the DA-MP.
2. If the problem persists, it is recommended to contact My Oracle Support.

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). This alarm is raised when a DA-MP is brought into service and a DA-MP configured DiamaterMaxMessageSize in DpiOption table value is greater than 16KB, but the available memory on DA-MP is less than 48GB.

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, it is recommended to contact My Oracle Support.

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:
eagleXgDiameterNoDaMpLeaderDetectedNotify

Recovery:

1. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25510 - Multiple DA-MP Leader Detected Alarm

Alarm Group:
DIAM

Description:
This alarm occurs when multiple active DA-MP leaders have been detected.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMultipleDaMpLeadersDetectedNotify

Recovery:

1. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25607 - DSR Signaling Firewall is administratively Disabled

Alarm Group
DIAM

Description
DSR Signaling Firewall is administratively Disabled

Severity
Minor

Instance
<System OAM name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterFwDisabledNotify

Recovery

1. Navigate to the Signaling Firewall page (**Main Menu** > **Diameter** > **Maintenance** > **Signaling Firewall**). Click the **Enable** button.
2. If the problem persists, it is recommended to contact My Oracle Support.

25608 - Abnormal DA-MP Firewall

Alarm Group
DIAM

Description
DSR Signaling Firewall Operational status is degraded.

Severity
Minor

Instance
<DA-MP name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterFwDegradedNotify

Recovery

1. Analyze event 25609 - Firewall Configuration Error encountered to identify the error(s) and the DA-MP which reported the error(s).
2. Analyze any platform alarms on the identified DA-MP. Follow the procedures to clear the platform alarms on the identified DA-MP
3. Disable the Signaling Firewall from the Signaling Firewall page (**Main Menu** > **Diameter** > **Maintenance** > **Signaling Firewall**).
4. If the alarm persists, restart the application on the identified DA-MP from the **Main Menu** > **Status & Manage** screen on the active Network OAM GUI.
5. If the problem is still unresolved, it is recommended to contact My Oracle Support for assistance.

25609 - Firewall Configuration Error encountered

Event Type
DIAM

Description
Firewall Configuration Error encountered

Severity
Info

Instance
<DA-MP name>

HA Score
Normal

Throttle Seconds
N/A

OID
eagleXgDiameterFwDisabledNotify

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for analysis and resolution.

25610 - DSR Signaling Firewall configuration inconsistency detected

Alarm Group
DIAM

Description
DSR Signaling Firewall configuration inconsistency detected

Severity
Minor

Instance
<DA-MP name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterFwDegradedNotify

Recovery

1. One possible cause could be manual changes in the "01dsr" domain of Linux firewall configuration on the DA-MP server. If so, the manual configuration should be rolled back.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25800 - Peer Discovery Failure

Alarm Group:
DIAM

Description:
Peer discovery failure.

Severity:
Minor

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has failed.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDpdRealmDiscoveryFailedNotify

Recovery:

1. Analyze event 25801 - Peer Discovery Configuration Error Encountered that has the same instance to identify the error(s).
2. Verify the DSR and DNS configurations and fix any configuration error(s).
3. Administratively refresh the Realm.
4. It is recommended to contact My Oracle Support for assistance.

25801 - Peer Discovery Configuration Error Encountered

Event Type:
DIAM

Description:
Peer discovery configuration error encountered.

Severity:
Info

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has encountered a configuration error.

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDpdConfigErrorNotify

Recovery:

1. Depending on the specific error code, follow the appropriate recovery steps.

Note: One likely cause is the number of instances of a managed object type is at capacity, and no new instances can be created. The user can delete unused instances of the MO type to free up capacity and try the Realm discovery again.

---

2. It is recommended to contact My Oracle Support for assistance.

25802 - Realm Expiration Approaching

Alarm Group:
DIAM

Description:
Realm expiration approaching.

Severity:
Minor, Major

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose expiry is approaching.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDpdConfigErrorNotify

Recovery:

1. Administratively disable the Realm.
2. Administratively extend the Realm.
3. Administratively refresh the Realm.
4. It is recommended to contact My Oracle Support for assistance.

25803 - Peer Discovery - Inconsistent Remote Host Port Assignment

Event Type:
DIAM

Description:
Peer discovery - inconsistent remote host port assignment.

Severity:
Info

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has encountered inconsistent remote host port assignment.

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDpdInconsistentPortAssignmentNotify

Recovery:

1. No action required. The DNS records for the Realm being discovered must be corrected by the Realm's DNS administrator.

25804 - Peer Discovery State Change

Event Type:
DIAM

Description:
Peer discovery state change.

Severity:
Info

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery state has changed.

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDpdInconsistentPortAssignmentNotify

Recovery:

1. No action required.

25805 - Invalid Shared TTG Reference

Alarm Group
DIAM

Description
Invalid Shared TTG Reference

Severity
Minor

Instance
<Route List Name>&<Route Group Name>&<TTG SG Name>&<TTG Name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterDoicInvalidSharedTtgRefNotify

Recovery

1. For the Route List named in the alarm instance, edit its configuration and delete the association to the non-existent Shared TTG. Then,
2. If desired, re-create the Shared TTG at its host site, and re-add the association to the Route List/Route Group.

> **Note:** Because, internally, the association of a TTG to the RL/RG is based on an internal ID, (not the TTG name), it is not valid to leave the original association in the Route List configuration and simply create a new Shared TTG with original name. This will not work, as the internal ID for the original TTG will not be the same as the ID for the new TTG (even though the TTG name is the same).

25806 - Invalid Internal SOAM Server Group Designation

Alarm Group
DIAM

Description
Invalid Internal SOAM Server Group Designation

Severity
Minor

Instance
<Route List Name>&<Route Group Name>&<TTG SG Name>&<TTG Name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterDoicInvalidInternalSoamSgDesignationNotify

Recovery

1. For the Route List named in the alarm instance, edit its configuration and delete the association to the Shared TTG. This will clear the alarm. The association can simply be re-added to restore integrity to the configuration.

31000-32800 - 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. No action is required. This event is used for command-line tool errors only.

31001 - S/W status

Alarm Group:
SW

Description:
Program status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolSwStatusNotify

Recovery:

1. No action required.

31002 - Process watchdog failure

Alarm Group:
SW

Description:
Process watchdog timed out.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolProcWatchdogFailureNotify

Recovery:

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

31003 - Tab thread watchdog failure

Alarm Group:
SW

Description:
Tab thread watchdog timed out

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolThreadWatchdogFailureNotify

Recovery:

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

31100 - Database replication fault

Alarm Group:
SW

Description:
The Database replication process is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. It is recommended to contact Customer Care Center.

31101 - Database replication to slave failure

Alarm Group:
REPL

Description:
Database replication to a slave database has failed. This alarm is generated when:

- The replication master finds the replication link is disconnected from the slave.
- The replication master's link to the replication slave is OOS, or the replication master cannot get the slave's correct HA state because of a failure to communicate.

- The replication mode is relayed in a cluster and either:
  - No nodes are active in cluster, or
  - None of the nodes in cluster are getting replication data.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepToSlaveFailureNotify

Recovery:

1. Verify the path for all services on a node by typing `path.test –a <toNode>` in a command interface to test the paths for all services.
2. Use the path test command to test the communication between nodes by typing `iqt -pE NodeInfo` to get the node ID. Then type `path.test -a <nodeid>` to test the paths for all services.
3. Examine the Platform savelogs on all MPs, SO, and NO by typing `sudo /usr/TKLC/plat/sbin/savelogs_plat` in the command interface. The plat savelogs are in the /tmp directory.
4. Check network connectivity between the affected servers.
5. If there are no issues with network connectivity, contact My Oracle Support.

31102 - Database replication from master failure

Alarm Group:
REPL

Description:
Database replication from a master database has failed. This alarm is generated when the replication slave finds the replication link is disconnected from the master.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepFromMasterFailureNotify

Recovery:

1. Verify the path for all services on a node by typing `path.test –a <toNode>` in a command interface to test the paths for all services.
2. Use the path test command to test the communication between nodes by typing `iqt -pE NodeInfo` to get the node ID. Then type `path.test -a <nodeid>` to test the paths for all services.
3. Examine the Platform savelogs on all MPs, SO, and NO by typing `sudo /usr/TKLC/plat/sbin/savelogs_plat` in the command interface. The plat savelogs are in the /tmp directory.
4. Indicates replication subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
5. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact My Oracle Support.

31103 - DB Replication update fault

Alarm Group:
REPL

Description:
Database replication process cannot apply update to DB.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepUpdateFaultNotify

Recovery:

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

31104 - DB Replication latency over threshold

Alarm Group:
REPL

Description:
Database replication latency has exceeded thresholds

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepLatencyNotify

Recovery:

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

31105 - Database merge fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeFaultNotify

Recovery:

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

31106 - Database merge to parent failure

Alarm Group:
COLL

Description:
Database merging to the parent Merge Node has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolDbMergeToParentFailureNotify

Recovery:

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

31107 - Database merge from child failure

Alarm Group:
COLL

Description:
Database merging from a child Source Node has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeFromChildFailureNotify

Recovery:

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

31108 - Database merge latency over threshold

Alarm Group:
COLL

Description:
Database Merge latency has exceeded thresholds

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeLatencyNotify

Recovery:

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

31109 - Topology config error

Alarm Group:
DB

Description:
Topology is configured incorrectly

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolTopErrorNotify

Recovery:

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

31110 - Database audit fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbAuditFaultNotify

Recovery:

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

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:

1. No action required.

31112 - DB replication update log transfer timed out

Alarm Group:
REPL

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
30

OID:
comcolDbRepUpLogTransTimeoutNotify

Recovery:

1. No action required.
2. It is recommended to contact My Oracle Support 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:

1. No action required.

31114 - DB replication over SOAP has failed

Alarm Group:
REPL

Description:
Database replication of configuration data via **SOAP** has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
3600

OID:
comcolDbReplicationSoapFaultNotify

Recovery:

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

31115 - Database service fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbServiceFaultNotify

Recovery:

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

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:

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

31117 - Low disk free

Alarm Group:
DISK

Description:
The amount of free disk is below configured thresholds

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolLowDiskFreeNotify

Recovery:

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

31118 - Database disk store fault

Alarm Group:
DISK

Description:
Writing the database to disk failed

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbDiskStoreFaultNotify

Recovery:

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

31119 - Database updatelog overrun

Alarm Group:
DB

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbUpdateLogOverrunNotify

Recovery:

1. This alarm indicates a replication audit transfer took too long to complete and the incoming update rate exceeded the engineered size of the update log. The system

will automatically retry the audit, and if successful, the alarm will clear and no further recovery steps are needed.

2. If the alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31120 - Database updatelog write fault

Alarm Group:
DB

Description:
A Database change cannot be stored in the updatelog

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbUpdateLogWriteFaultNotify

Recovery:

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

31121 - Low disk free early warning

Alarm Group:
DISK

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolLowDiskFreeEarlyWarningNotify

Recovery:

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

31122 - Excessive shared memory early warning

Alarm Group:
MEM

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

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

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:

1. 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:

1. It is recommended to contact My Oracle Support.

31125 - Database durability degraded

Alarm Group:
REPL

Description:
Database durability has dropped below configured durability level

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbDurabilityDegradedNotify

Recovery:

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

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:

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

31127 - DB Replication Audit Complete

Alarm Group:
REPL

Description:
DB replication audit completed

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepAuditCompleteNotify

Recovery:

1. No action required.

31128 - ADIC Found Error

Alarm Group:
REPL

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbADICErrorNotify

Recovery:

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

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:

1. No action required.

31130 - Network health warning

Alarm Group:
NET

Description:
Network health issue detected

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolNetworkHealthWarningNotify

Recovery:

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

31131 - DB Ousted Throttle Behind

Alarm Group:
DB

Description:
DB ousted throttle may be affecting processes.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolOustedThrottleWarnNotify

Recovery:

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

31132 - DB Replication Precedence Relaxed

Event Type
REPL

Description
Standby Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Databases to update as fast as possible.

Severity
Info

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Throttle Seconds
150

OID
comcolDbRepPrecRelaxedNotify

Recovery

1. No action required.

31133 - DB Replication Switchover Exceeds Threshold

Alarm Group
REPL

Description
DB Replication Active to Standby switchover exceeded maximum switchover time.

Severity
Major

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbRepSwitchoverNotify

Recovery

1. If this alarm is raised, it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If the problem persists, it is recommended to contact My Oracle Support.

31134 - DB Site Replication To Slave Failure

Alarm Group
REPL

Description
DB Site replication to a slave DB has failed.

Severity
Minor

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbSiteRepToSlaveFailureNotify

Recovery

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

31135 - DB Site Replication From Master Failure

Alarm Group
REPL

Description
DB Site replication from a master DB has failed.

Severity
Minor

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbSiteRepFromMasterFailureNotify

Recovery

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

31136 - DB Site Replication Precedence Relaxed

Event Type
REPL

Description
Standby Site Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Site Databases to update as fast as possible.

Severity
Info

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Throttle Seconds
150

OID
comcolDbSiteRepPrecRelaxedNotify

Recovery

1. No action required.

31137 - DB Site Replication Latency Over Threshold

Alarm Group
REPL

Description
DB Site Replication latency has exceeded thresholds.

Severity
Major

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbSiteRepLatencyNotify

Recovery

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

31140 - Database perl fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbPerlFaultNotify

Recovery:

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

31145 - Database SQL fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbSQLFaultNotify

Recovery:

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

31146 - DB mastership fault

Alarm Group:
SW

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMastershipFaultNotify

Recovery:

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

31147 - DB upsynclog overrun

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbUpSyncLogOverrunNotify

Recovery:

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

31148 - DB lock error detected

Alarm Group:
DB

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbLockErrorNotify

Recovery:

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

31149 - DB Late Write Nonactive

Alarm Group
DB

Description
Application wrote to database while HA role change from active was in progress.

Severity
Minor

Instance
HA resource name

HA Score
Normal

Auto Clear Seconds
3600

OID
comcolDbLateWriteNotify

Recovery

1. It is recommended to contact My Oracle Support for assistance.

31200 - Process management fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcMgmtFaultNotify

Recovery:

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

31201 - Process not running

Alarm Group:
PROC

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcNotRunningNotify

Recovery:

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

31202 - Unkillable zombie process

Alarm Group:
PROC

Description:
A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcZombieProcessNotify

Recovery:

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

31206 - Process mgmt monitoring fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcMgmtMonFaultNotify

Recovery:

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

31207 - Process resource monitoring fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcResourceMonFaultNotify

Recovery:

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

31208 - IP port server fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolPortServerFaultNotify

Recovery:

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

31209 - Hostname lookup failed

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHostLookupFailedNotify

Recovery:

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

31213 - Process scheduler fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcSchedulerFaultNotify

Recovery:

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

31214 - Scheduled process fault

Alarm Group:
PROC

Description:
A scheduled process cannot be executed or abnormally terminated

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolScheduleProcessFaultNotify

Recovery:

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

31215 - Process resources exceeded

Alarm Group:
SW

Description:
A process is consuming excessive system resources.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
14400

OID:
comcolProcResourcesExceededFaultNotify

Recovery:

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

31216 - SysMetric configuration error

Alarm Group:
SW

Description:
A SysMetric Configuration table contains invalid data

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolSysMetricConfigErrorNotify

Recovery:

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

31217 - Network Health Warning

Alarm Group
SW

Description
Missed Heartbeats Detected

Severity
Minor

Instance
IP Address

HA Score
Normal

Auto Clear Seconds
300

OID
comcolNetworkHealthWarningNotify

Recovery

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

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:

1. It is recommended to contact My Oracle Support.

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:

1. It is recommended to contact My Oracle Support.

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:

1. It is recommended to contact My Oracle Support.

31223 - HA Heartbeat transmit failure

Alarm Group:
HA

Description:
The high availability monitor failed to send heartbeat.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaHbTransmitFailureNotify

Recovery:

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

31224 - HA configuration error

Alarm Group:
HA

Description:
High availability configuration error

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaCfgErrorNotify

Recovery:

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

31225 - HA service start failure

Alarm Group:
HA

Description:
The required high availability resource failed to start.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0

OID:
comcolHaSvcStartFailureNotify

Recovery:

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

31226 - HA availability status degraded

Alarm Group:
HA

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0

OID:
comcolHaAvailDegradedNotify

Recovery:

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

31227 - HA availability status failed

Alarm Group:
HA

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
comcolHaAvailFailedNotify

Recovery:

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

31228 - HA standby offline

Alarm Group:
HA

Description:
High availability standby server is offline.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolHaStandbyOfflineNotify

Recovery:

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

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:

1. Status message - no action required.

31230 - Recent alarm processing fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolRecAlarmEvProcFaultNotify

Recovery:

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

31231 - Platform alarm agent fault

Alarm Group:
SW

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolPlatAlarmAgentNotify

Recovery:

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

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:

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

31233 - HA Path Down

Alarm Group:
HA

Description:
High availability path loss of connectivity

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaPathDownNotify

Recovery:

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

31234 - Untrusted Time Upon Initialization

Alarm Group:
REPL

Description:
Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolUtrustedTimeOnInitNotify

Recovery:

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

31235 - Untrusted Time After Initialization

Alarm Group:
REPL

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolUtrustedTimePostInitNotify

Recovery:

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

31236 - HA Link Down

Alarm Group:
HA

Description:
High availability TCP link is down.

Severity:
Critical

Instance:
Remote node being connected to plus the path identifier

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaLinkDownNotify

Recovery:

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

31240 - Measurements collection fault

Alarm Group:
SW

Description:
The measurements collector (statclerk) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolMeasCollectorFaultNotify

Recovery:

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

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:

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

31260 - SNMP Agent

Alarm Group:
SW

Description:
The SNMP agent (cmsnmpa) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
DbcomcolSnmpAgentNotify

Recovery:

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

31261 - SNMP Configuration Error

Alarm Group
SW

Description
A SNMP configuration error was detected

Severity
Minor

Instance
comcolAlarmSrcNode, comcolAlarmNumber, comcolAlarmInstance, comcolAlarmSeverity, comcolAlarmText, comcolAlarmInfo, comcolAlarmGroup, comcolServerHostname, comcolAlarmSequence, comcolAlarmTimestamp, comcolAlarmEventType, comcolAlarmProbableCause, comcolAlarmAdditionalInfo

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
comcolSnmpConfigNotify

Recovery

1. Export event history for the given server and all processes.
2. It is recommended to contact My Oracle Support for assistance.

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:

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

31280 - HA Active to Standby transition

Alarm Group:
HA

Description:
HA active to standby activity transition

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolActiveToStandbyTransNotify

Recovery:

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

31281 - HA Standby to Active transition

Alarm Group:
HA

Description:
HA standby to active activity transition

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolStandbyToActiveTransNotify

Recovery:

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

31282 - HA Management Fault

Alarm Group:
HA

Description:
The HA manager (cmha) is impaired by a software fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaMgmtFaultNotify

Recovery:

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

31283 - Lost Communication with server

Alarm Group:
HA

Description:
Highly available server failed to receive mate heartbeats

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolHaServerOfflineNotify

Recovery:

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

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Group:
HA

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRemoteHeartbeatWarningNotify

Recovery:

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

31285 - HA Node Join Recovery Entry

Alarm Group:
HA

Description:
High availability **node join** recovery entered

Severity:
Info

Instance:
Cluster set key of the DC outputting the event

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaSbrEntryNotify

Recovery:

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

31286 - HA Node Join Recovery Plan

Alarm Group:
HA

Description:
High availability node join recovery plan

Severity:
Info

Instance:
Names of HA Policies (as defined in HA policy configuration)

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaSbrPlanNotify

Recovery:

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

31287 - HA Node Join Recovery Complete

Alarm Group:
HA

Description:
High availability node join recovery complete

Severity:
Info

Instance:
Names of HA Policies (as defined in HA policy configuration)

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaSbrCompleteNotify

Recovery:

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

31288 - HA Site Configuration Error

Alarm Group
HA

Description
High availability site configuration error

Severity
Critical

Instance
GroupName, Policy ID, Site Name

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
comcolHaBadSiteCfgNotify

Recovery

1. If this alarm does not clear after correcting the configuration, it is recommended to contact My Oracle Support for assistance.

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

31291 - HA Election Status

Alarm Group:
HA

Description:
HA DC Election status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaElectionStatusNotify

Recovery:

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

31292 - HA Policy Status

Alarm Group:
HA

Description:
HA Policy plan status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaPolicyStatusNotify

Recovery:

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

31293 - HA Resource Link Status

Alarm Group:
HA

Description:
This alarm is raised for nodes in our topology that we should be connected to (i.e., not OOS), but that we do not have any TCP links to it over any configured paths. It does not matter why the links were not established (networking connectivity, node not running, etc.).

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaLinkStatusNotify

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.
3. If the problem persists, it is recommended to contact My Oracle Support.

31294 - HA Resource Status

Alarm Group:
HA

Description:
HA Resource registration status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaResourceStatusNotify

Recovery:

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

31295 - HA Action Status

Alarm Group:
HA

Description:
HA Resource action status

Severity:
Info

Instance
N/A

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaActionStatusNotify

Recovery:

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

31296 - HA Monitor Status

Alarm Group:
HA

Description:
HA Monitor action status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaMonitorStatusNotify

Recovery:

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

31297 - HA Resource Agent Info

Alarm Group:
HA

Description:
HA Resource Agent Info

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaInfoNotify

Recovery:

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

31298 - HA Resource Agent Detail

Alarm Group:
HA

Description:
Resource Agent application detailed information

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaDetailNotify

Recovery:

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

31299 - HA Notification Status

Alarm Group:
HA

Description:
HA Notification status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaNotificationNotify

Recovery:

1. 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:

1. No action required.

31301 - HA Topology Events

Alarm Group:
HA

Description:
HA Topology events

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrHaTopologyNotify

Recovery:

1. No action required.

31322 - HA Configuration Error

Alarm Group
HA

Description
High availability configuration error

Severity
Minor

Instance
NodeID, or HA Tunnel ID

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
comcolHaBadCfgNotify

Recovery

1. It is recommended to contact My Oracle Support.

32100 - Breaker Panel Feed Unavailable

Alarm Group:
PLAT

Description:
Breaker Panel Breaker Unavailable

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlFeedUnavailable

Recovery:

1. It is recommended to contact My Oracle Support to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Group:
PLAT

Description:
Breaker Panel Breaker Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlBreakerFailure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

Alarm Group:
PLAT

Description:
Breaker Panel Monitoring Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlMntFailure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32103 - Power Feed Unavailable

Alarm Group:
PLAT

Description:
Power Feed Unavailable

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerFeedUnavail

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Group:
PLAT

Description:
Power Supply 1 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply1Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Group:
PLAT

Description:
Power Supply 2 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply2Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group:
PLAT

Description:
Power Supply 3 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply3Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32107 - Raid Feed Unavailable

Alarm Group:
PLAT

Description:
Raid Feed Unavailable

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidFeedUnavailable

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Group:
PLAT

Description:
Raid Power 1 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidPower1Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Group:
PLAT

Description:
Raid Power 2 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidPower2Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Group:
PLAT

Description:
Raid Power 3 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidPower3Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32111 - Device Failure

Alarm Group:
PLAT

Description:
Device Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceFailure

Recovery:

1. It is recommended to contact My Oracle Support to request hardware replacement.

32112 - Device Interface Failure

Alarm Group:
PLAT

Description:
Device Interface Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceIfFailure

Recovery:

1. It is recommended to contact My Oracle Support to request hardware replacement.

32113 - Uncorrectable ECC memory error

Alarm Group:
PLAT

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdEccUncorrectableError

Alarm ID:
TKSPLATCR14

Recovery:

1. Contact the hardware vendor to request hardware replacement.

32114 - SNMP get failure

Alarm Group:
PLAT

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSNMPGetFailure

Alarm ID:
TKSPLATCR15

Recovery:

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

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Group:
PLAT

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDaemonNotSynchronizedFailure

Alarm ID:
TKSPLATCR16

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
   a. Ensure ntpd service is running with correct options: -x -g.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Type `/usr/sbin/ntpdc -c sysinfo` to check the current state of the ntpd daemon.
   d. Verify the ntp peer configuration; execute ntpq -np; and analyze the output. Verify peer data, such as tally code (first column before remote), remote, refid, stratum (st), and jitter, are valid for server.

e. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server, then ping the ntp peer to determine if peer can be reached.

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

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

a. Reset ntpd:

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

4. Conform to recommended NTP topology and strategy.
   - No fewer than tree references are recommended.
   - If selecting a different number, the number should be odd.
   - No intermediate reference should be a virtualized server.
   - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact My Oracle Support.

32116 - TPD Server's Time Has Gone Backwards

Alarm Group:
PLAT

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPTimeGoneBackwards

Alarm ID:
TKSPLATCR17

Recovery:

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

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. Reset ntpd:
   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start
4. Conform to recommended NTP topology and strategy.
   - No fewer than tree references are recommended.
   - If selecting a different number, the number should be odd.
   - No intermediate reference should be a virtualized server.
   - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact My Oracle Support.

32117 - TPD NTP Offset Check Failure

Alarm Group:
PLAT

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

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpOffsetCheckFailure

Alarm ID:
TKSPLATCR18

Recovery:

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

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop

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

4. Conform to recommended NTP topology and strategy.
   - No fewer than tree references are recommended.
   - If selecting a different number, the number should be odd.
   - No intermediate reference should be a virtualized server.
   - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact My Oracle Support.

32300 - Server fan failure

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFanError

Alarm ID:
TKSPLATMA1

Recovery:

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

32301 - Server internal disk error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdIntDiskError

Alarm ID:
TKSPLATMA2

Recovery:

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

   ```
   cat /proc/mdstat

   cat /etc/raidtab
   ```

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

32303 - Server Platform error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPlatformError

Alarm ID:
TKSPLATMA4

Recovery:

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

   ```
   cat /proc/mdstat

   cat /etc/raidtab
   ```

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

32304 - Server file system error

Alarm Group:
PLAT

Description:
This alarm indicates unsuccessful writing to at least one of the server's file systems.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFileSystemError

Alarm ID:
TKSPLATMA5

Recovery:

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

32305 - Server Platform process error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPlatProcessError

Alarm ID:
TKSPLATMA6

Recovery:

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

32306 - Server RAM shortage error

Alarm Group:
PLAT

Description:
Not Implemented.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRamShortageError

Recovery

1. It is recommended to contact My Oracle Support.

32307 - Server swap space shortage failure

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwapSpaceShortageError

Alarm ID:
TKSPLATMA8

Recovery:

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

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

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

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

32308 - Server provisioning network error

Alarm Group:
PLAT

Description:
This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdProvNetworkError

Alarm ID:
TKSPLATMA9

Recovery:

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

32312 - Server disk space shortage error

Alarm Group:
PLAT

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

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskSpaceShortageError

Alarm ID:
TKSPLATMA13

Recovery:

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

32313 - Server default route network error

Alarm Group:
PLAT

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

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDefaultRouteNetworkError

Recovery:

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

32314 - Server temperature error

Alarm Group:
PLAT

Description:
The internal temperature within the server is unacceptably high.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerTemperatureError

Alarm ID:
TKSPLATMA15

Recovery:

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

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

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

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

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

32315 - Server mainboard voltage error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerMainboardVoltageError

Alarm ID:
TKSPLATMA16

Recovery:

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

32316 - Server power feed error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerFeedError

Alarm ID:
TKSPLATMA17

Recovery:

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

32317 - Server disk health test error

Alarm Group:
PLAT

Description:
Either the hard drive has failed or failure is imminent.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskHealthError

Alarm ID:
TKSPLATMA18

Recovery:

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

32318 - Server disk unavailable error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskUnavailableError

Alarm ID:
TKSPLATMA19

Recovery:

1. Run syscheck in verbose mode.

2. It is recommended to contact My Oracle Support and provide the system health check output.

32320 - Device interface error

Alarm Group:
PLAT

Description:
This alarm indicates that the IP bond is either not configured or down.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceIfError

Alarm ID:
TKSPLATMA21

Recovery:

1. Run syscheck in verbose mode.
2. Investigate the failed bond, and slave devices, configuration:
   a. Navigate to /etc/sysconfig/network-scripts for the persistent configuration of a device.
3. Determine if the failed bond, and slave devices, has been administratively shut down or has operational issues:
   a. cat /proc/net/bonding/bondX, where X is bond designation
   b. ethtool <slave device>
4. If bond, and slaves, are healthy attempt to administratively bring bond up:
   a. ifup bondX
5. If the problem has not been resolved, it is recommended to contact My Oracle Support and provide the system health check output and the output of the above investigation.

32321 - Correctable ECC memory error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdEccCorrectableError

Alarm ID:
TKSPLATMA22

Recovery:

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

32322 - Power Supply A error

Alarm Group:
PLAT

Description:
This alarm indicates that power supply 1 (feed A) has failed.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply1Error

Alarm ID:
TKSPLATMA23

Recovery:

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

32323 - Power Supply B error

Alarm Group:
PLAT

Description:
This alarm indicates that power supply 2 (feed B) has failed.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply2Error

Alarm ID:
TKSPLATMA24

Recovery:

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

32324 - Breaker panel feed error

Alarm Group:
PLAT

Description:
This alarm indicates that the server is not receiving information from the breaker panel relays.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlFeedError

Alarm ID:
TKSPLATMA25

Recovery:

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

32325 - Breaker panel breaker error

Alarm Group:
PLAT

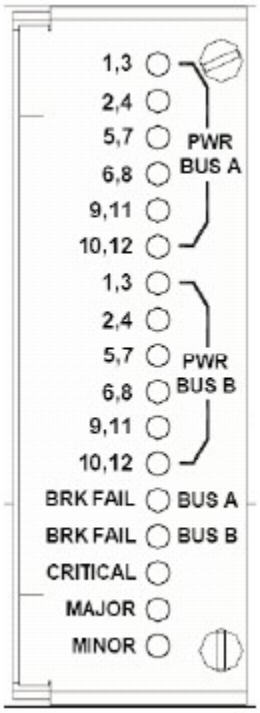
Description:
This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see Figure 3-4) identify whether the fault occurred on the input power or the output power, as follows:

- 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 3-4 Breaker Panel LEDs



Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
TPDBrkPnlBreakerError

Alarm ID:
TKSPLATMA26

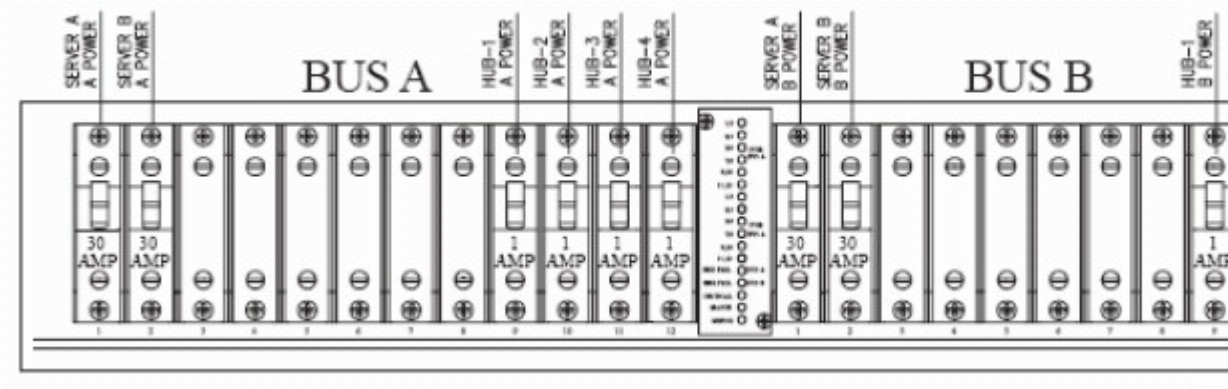
Recovery:

1. Verify that the same alarm is displayed by both servers. The single breaker panel normally sends alarm information to both servers:

   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by both servers, go to the next step.

2. For each breaker assignment, verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

Figure 3-5 Breaker Panel Setting



If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Perform the following steps to correct this problem:

- Verify that the customer provided source for the affected power feed is operational. If the power source is properly functioning, have an electrician remove the plastic cover from the rear of the breaker panel and verify the power source is indeed connected to the input power feed connector on the rear of the breaker panel. Correct any issues found.
- Check the LEDs in the PWR BUS A group and the PWR BUS B group again.

  a. If the LEDs are now illuminated Green, the issue has been resolved. Proceed to step 4 to verify that the alarm has been cleared.

  b. If the LEDs are still illuminated Red, continue to the next sub-step.

- Have the electrician verify the integrity of the input power feed. The input voltage should measure nominally -48VDC (that is, between -41VDC and -60VDC). If the supplied voltage is not within the acceptable range, the input power source must be repaired or replaced.

Note:

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

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

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

  a. If the LEDs are now illuminated Green, the issue has been resolved and proceed to step 4 to verify that the alarm has been cleared.

  b. If the LEDs are still illuminated Red, skip to step 5

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

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

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

   b. After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, run syscheck and contact My Oracle Support

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

5. Run syscheck.

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

32326 - Breaker panel monitoring error

Alarm Group:
PLAT

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

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

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

until the Breaker Panel Monitoring Error has been corrected.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlMntError

Alarm ID:
TKSPLATMA27

Recovery:

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

32327 - Server HA Keepalive error

Alarm Group:
PLAT

Description:
This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaKeepaliveError

Alarm ID:
TKSPLATMA28

Recovery:

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

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

4. It is recommended to contact My Oracle Support.

32331 - HP disk problem

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskProblem

Alarm ID:
TKSPLATMA32

Recovery:

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

32332 - HP Smart Array controller problem

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskCtrlrProblem

Alarm ID:
TKSPLATMA33

Recovery:

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

32333 - HP hpacucliStatus utility problem

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHPACUCLIProblem

Alarm ID:
TKSPLATMA34

Recovery:

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

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

   a. Executing "status TPDhpDiskStatus", or "status TKLChpacucli" depending on TPD release, should produce output indicating that the process is running.

4. If not running, attempt to start the HP disk status process :

   "start TPDhpDiskStatus", or if appropriate "start TKLChpacucli" .

5. Verify that there are no hpssacli, or hpacucli, error messages in /var/log/messages. If there are this could indicate that the HP utility is hung. If the HP hpssacli utility, or hpacucli utility, is hung, proceed with next step.
6. It is recommended to contact My Oracle Support and provide the system health check output, and savelogs_plat output.

32335 - Switch link down error

Alarm Group:
PLAT

Description:
The link is down.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwitchLinkDownError

Alarm ID:
TKSPLATMA36

Recovery:

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

32336 - Half Open Socket Limit

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHalfOpenSockLimit

Alarm ID:
TKSPLATMA37

Recovery:

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

32337 - Flash Program Failure

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFlashProgramFailure

Alarm ID:
TKSPLATMA38

Recovery:

1. It is recommended to contact My Oracle Support.

32338 - Serial Mezzanine Unseated

Alarm Group:
PLAT

Description:
This alarm indicates that a connection to the serial mezzanine board may not be properly seated.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSerialMezzUnseated

Alarm ID:
TKSPLATMA39

Recovery:

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

32339 - TPD Max Number Of Running Processes Error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMaxPidLimit

Alarm ID:
TKSPLATMA40

Recovery:

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

32340 - TPD NTP Daemon Not Synchronized Error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDaemonNotSynchronizedError

Alarm ID:
TKSPLATMA41

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.

c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.

d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.

2. If ntp peer is reachable, restart the ntpd service.

3. If problem persists then a reset the NTP date may resolve the issue.

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

a. To reset date:

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

4. If the problem persists, it is recommended to contact My Oracle Support.

32341 - TPD NTP Daemon Not Synchronized Error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDaemonNeverSynchronized

Alarm ID:
TKSPLATMA42

Recovery:

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

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

   a. To reset date:

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

4. If the problem persists, it is recommended to contact My Oracle Support.

32342 - NTP Offset Check Error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpOffsetCheckError

Alarm ID:
TKSPLATMA43

Recovery:

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

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

   a. To reset date:

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

4. If the problem persists, it is recommended to contact My Oracle Support.

32343 - TPD RAID disk

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskProblem

Alarm ID:
TKSPLATMA44

Recovery:

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

32344 - TPD RAID controller problem

Alarm Group:
PLAT

Description:
This alarms indicates that RAID controller needs intervention.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskCtrlrProblem

Alarm ID:
TKSPLATMA45

Recovery:

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

32345 - Server Upgrade snapshot(s) invalid

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdUpgradeSnapshotInvalid

Alarm ID:
TKSPLATMA46

Recovery:

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

32346 - OEM hardware management service reports an error

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdOEMHardware

Alarm ID:
TKSPLATMA47

Recovery:

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

32347 - The hwmgmtcliStatus daemon needs intervention

Alarm Group:
PLAT

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

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHWMGMTCLIProblem

Alarm ID:
TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the hwmgmtd process is running. If not running verify that it was not administratively stopped.
   - Executing "service hwmgmtd status" should produce output indicating that the process is running.
   - If not running attempt to start process "service hwmgmtd status".
4. Determine if the TKLChwmgmtcli process is running. If not running verify that it was not administratively stopped.

- Executing "status TKLChwmgmtcli" should produce output indicating that the process is running.
- If not running attempt to start process "start TKLChwmgmtcli".

5. Verify that there are no hwmgmt error messages in /var/log/messages. If there are this could indicate that the Oracle utility is hung. If hwmgmtd process is hung, proceed with next step.
6. It is recommended to contact My Oracle Support and provide the system health check output.

32348 - FIPS subsystem problem

Alarm Group:
PLAT

Description:
This alarm indicates the **FIPS** subsystem is not running or has encountered errors.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFipsSubsystemProblem

Recovery:

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

32349 - File Tampering

Alarm Group:
PLAT

Description:
This alarm indicates **HIDS** has detected file tampering.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHidsFileTampering

Recovery:

1. It is recommended to contact My Oracle Support.

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:

1. It is recommended to contact My Oracle Support.

32500 - Server disk space shortage warning

Alarm Group:
PLAT

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

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskSpaceShortageWarning

Alarm ID:
TKSPLATMI1

Recovery:

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

32501 - Server application process error

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdApplicationProcessError

Alarm ID:
TKSPLATMI2

Recovery:

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

32502 - Server hardware configuration error

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHardwareConfigError

Alarm ID:
TKSPLATMI3

Recovery:

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

32505 - Server swap space shortage warning

Alarm Group:
PLAT

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

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwapSpaceShortageWarning

Alarm ID:
TKSPLATMI6

Recovery:

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

32506 - Server default router not defined

Alarm Group:
PLAT

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

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDefaultRouteNotDefined

Alarm ID:
TKSPLATMI7

Recovery:

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

3. If the alarm has not cleared, it is recommended to collect the syscheck output and contact My Oracle Support.

32507 - Server temperature warning

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerTemperatureWarning

Alarm ID:
TKSPLATMI8

Recovery:

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

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

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

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

5. Run syscheck.

6. If the problem has not been resolved, it is recommended to contact My Oracle Support.

32508 - Server core file detected

Alarm Group:
PLAT

Description:
This alarm indicates that an application process has failed and debug information is available.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerCoreFileDetected

Alarm ID:
TKSPLATMI9

Recovery:

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

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

   Add the command output to the service request. Include the date of creation found in the command output.
3. Attach core files to the My Oracle Support service request.
4. The user can remove the files to clear the alarm with this command:

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

32509 - Server NTP Daemon not synchronized

Alarm Group:
PLAT

Description:
This alarm indicates that the **NTP daemon** (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDeamonNotSynchronizedWarning

Alarm ID:
TKSPLATMI10

Recovery:

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

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

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

4. If the problem persists, it is recommended to contact My Oracle Support.

32510 - CMOS battery voltage low

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdCMOSBatteryVoltageLow

Alarm ID:
TKSPLATMI11

Recovery:

1. It is recommended to contact My Oracle Support.

32511 - Server disk self test warning

Alarm Group:
PLAT

Description:
A non-fatal disk issue (such as a sector cannot be read) exists.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSmartTestWarn

Alarm ID:
TKSPLATMI12

Recovery:

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

32512 - Device warning

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceWarn

Alarm ID:
TKSPLATMI13

Recovery:

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

32513 - Device interface warning

Alarm Group:
PLAT

Description:
This alarm can be generated by either an SNMP trap or an IP bond error.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceIfWarn

Alarm ID:
TKSPLATMI14

Recovery:

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

32514 - Server reboot watchdog initiated

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdWatchdogReboot

Alarm ID:
TKSPLATMI15

Recovery:

1. It is recommended to contact My Oracle Support.

32515 - Server HA failover inhibited

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaInhibited

Alarm ID:
TKSPLATMI16

Recovery:

1. It is recommended to contact My Oracle Support.

32516 - Server HA Active to Standby transition

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaActiveToStandbyTrans

Alarm ID:
TKSPLATMI17

Recovery:

1. It is recommended to contact My Oracle Support.

32517 - Server HA Standby to Active transition

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaStandbyToActiveTrans

Alarm ID:
TKSPLATMI18

Recovery:

1. It is recommended to contact My Oracle Support.

32518 - Platform Health Check failure

Alarm Group:
PLAT

Description:
This alarm is used to indicate a configuration error.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHealthCheckFailed

Alarm ID:
TKSPLATMI19

Recovery:

1. It is recommended to contact My Oracle Support.

32519 - NTP Offset Check failure

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpOffsetCheckWarning

Alarm ID:
TKSPLATMI20

Recovery:

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

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

> **Note:** Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

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

4. If the problem persists, it is recommended to contact My Oracle Support.

32520 - NTP Stratum Check failure

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpStratumCheckFailed

Alarm ID:
TKSPLATMI21

Recovery:

1. Verify NTP settings and that NTP sources can be reached.

   a. Ensure ntpd service is running.

   b. Verify the content of the /etc/ntp.conf file is correct for the server.

c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.

d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.

2. If ntp peer is reachable, restart the ntpd service.

3. If problem persists then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

a. To reset date:

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

4. If the problem persists, it is recommended to contact My Oracle Support.

32521 - SAS Presence Sensor Missing

Alarm Group:
PLAT

Description:
This alarm indicates that the T1200 server drive sensor is not working.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sasPresenceSensorMissing

Alarm ID:
TKSPLATMI22

Recovery:

1. It is recommended to contact My Oracle Support to get a replacement sensor.

32522 - SAS Drive Missing

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sasDriveMissing

Alarm ID:
TKSPLATMI23

1. It is recommended to contact My Oracle Support.

32524 - HP disk resync

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskResync

Alarm ID:
TKSPLATMI25

Recovery:

1. Run syscheck in verbose mode.
2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck.
3. If the alarm persists, it is recommended to contact My Oracle Support and provide the syscheck output.

32525 - Telco Fan Warning

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdTelcoFanWarning

Alarm ID:
TKSPLATMI26

Recovery:

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

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

32526 - Telco Temperature Warning

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdTelcoTemperatureWarning

Alarm ID:
TKSPLATMI27

Recovery:

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

32527 - Telco Power Supply Warning

Alarm Group:
PLAT

Description:
This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdTelcoPowerSupplyWarning

Alarm ID:
TKSPLATMI28

Recovery:

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

32528 - Invalid BIOS value

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdInvalidBiosValue

Alarm ID:
TKSPLATMI29

Recovery:

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

32529 - Server Kernel Dump File Detected

Alarm Group:
PLAT

Description:
This alarm indicates that the kernel has crashed and debug information is available.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerKernelDumpFileDetected

Alarm ID:
TKSPLATMI30

Recovery:

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

32530 - TPD Upgrade Failed

Alarm Group:
PLAT

Description:
This alarm indicates that a TPD upgrade has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
TpdServerUpgradeFailed

Alarm ID:
TKSPLATMI31

Recovery:

1. It is recommended to contact My Oracle Support.

32531 - Half Open Socket Warning Limit

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHalfOpenSocketWarning

Alarm ID:
TKSPLATMI32

Recovery:

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

32532 - Server Upgrade Pending Accept/Reject

Alarm Group:
PLAT

Description:
This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerUpgradePendingAccept

Alarm ID:
TKSPLATMI33

Recovery:

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

32533 - TPD Max Number Of Running Processes Warning

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMaxPidWarning

Alarm ID:
TKSPLATMI34

Recovery:

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

32534 - TPD NTP Source Is Bad Warning

Alarm Group:
PLAT

Description:
This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPSourceIsBad

Alarm ID:
TKSPLATMI35

Recovery:

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

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:
   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start
4. If the problem persists, it is recommended to contact My Oracle Support.

32535 - TPD RAID disk resync

Alarm Group:
PLAT

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

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskResync

Alarm ID:
TKSPLATMI36

Recovery:

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

32536 - TPD Server Upgrade snapshot(s) warning

Alarm Group:
PLAT

Description:
This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdUpgradeSnapshotWarning

Alarm ID:
TKSPLATMI37

Recovery:

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

32538 - Platform Data Collection Error

Alarm Group
PLAT

Description
Platform Data Collection Error

Severity
Minor

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

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
tpdPdcError

Recovery

1. Run `/usr/TKLC/plat/bin/pdcAdm`. If ran as admusr, use sudo to run the command.
2. If this command fails, it is recommended to collect the output and contact My Oracle Support.

32539 - Server Patch Pending Accept/Reject

Alarm Group
PLAT

Description
Server Patch Pending Accept/Reject

Severity
Minor

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

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
tpdServerPatchPendingAccept

Recovery

1. Accept or reject the patch per the application documentation procedure.

32540 - CPU Power limit mismatch

Alarm Group:
PLAT

Description:
The BIOS setting for CPU Power Limit is different than expected.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdCpuPowerLimitMismatch

Alarm ID:
TKSPLATMI41

Recovery:

1. It is recommended to contact My Oracle Support.

32700 - Telco Switch Notification

Alarm Group:
PLAT

Description
Telco Switch Notification

Severity
Info

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

HA Score
Normal

Auto Clear Seconds
86400

OID
tpdTelcoSwitchNotification

Recovery:

1. It is recommended to contact My Oracle Support.

32701 - HIDS Initialized

Alarm Group:
PLAT

Description:
This alarm indicates HIDS was initialized.

Default Severity:
Info

OID:
tpdHidsBaselineCreated

Recovery:

1. It is recommended to contact My Oracle Support.

32702 - HIDS Baseline Deleted

Alarm Group:
PLAT

Description:
HIDS baseline was deleted.

Default Severity:
Info

OID:
tpdHidsBaselineDeleted

Recovery:

1. It is recommended to contact My Oracle Support.

32703 - HIDS Enabled

Alarm Group:
PLAT

Description:
HIDS was enabled.

Default Severity:
Info

OID:
tpdHidsEnabled

Recovery:

1. It is recommended to contact My Oracle Support.

32704 - HIDS Disabled

Alarm Group:
PLAT

Description:
HIDS was disabled.

Default Severity:
Info

OID:
tpdHidsDisabled

Recovery:

1. It is recommended to contact My Oracle Support.

32705 - HIDS Monitoring Suspended

Alarm Group:
PLAT

Description:
HIDS monitoring suspended.

Default Severity:
Info

OID:
tpdHidsSuspended

Recovery:

1. It is recommended to contact My Oracle Support.

32706 - HIDS Monitoring Resumed

Alarm Group:
PLAT

Description:
HIDS monitoring resumed.

Default Severity:
Info

OID:
tpdHidsResumed

Recovery:

1. It is recommended to contact My Oracle Support.

32707 - HIDS Baseline Updated

Alarm Group:
PLAT

Description:
HIDS baseline updated.

Default Severity:
Info

OID:
tpdHidsBaselineUpdated

Recovery:

1. It is recommended to contact My Oracle Support.

4

Key Performance Indicators (KPIs)

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

General KPIs information

This section provides general information about KPIs and lists the KPIs that can be viewed from the **Status & Manage** > **KPIs** page.

KPIs overview

Key Performance Indicators (KPIs) allow you 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.

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.

Communication Agent (ComAgent) KPIs

The KPI values associated with **ComAgent** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 4-1 Communication Agent KPIs

Variable	Description
User Data Ingress message rate	The number of User Data Stack Events received by ComAgent.

Table 4-1 (Cont.) Communication Agent KPIs

Variable	Description
Broadcast Data Rate	The overall data broadcast rate on the server.

Connection Maintenance KPIs

The KPI values associated with Connection Maintenance are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 4-2 Connection Maintenance KPIs

Variable	Description
RxConnAvgMPS	Exponentially smoothed average rate in MPS on the connection. Note: This measurement will be sampled periodically and reported in the Connections Maintenance GUI as a type of KPI.

Diameter (DIAM) KPIs

The KPI values associated with **Diameter** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 4-3 DIAM KPIs

Variable	Description
MsgCopyTxQueueUtilization	Percentage of utilization of the **Message Copy** Tx Queue
Average Response Time	The average time from when routing receives a request message from a peer to when routing sends an answer message to that peer.
Transaction Success Rate	Percentage of Diameter and RADIUS transactions successfully completed on a DA-MP server with respect to the offered load.

KPIs server elements

This table describes KPIs that appear regardless of server role.

Table 4-4 KPIs Server Elements

KPIs Status Element	Description
Network Element	The network element name (set up on the **Configuration** > **Network Elements** page) associated with each Server Hostname.
Server Hostname	The server hostname set up on the **Configuration** > **Servers** page. All servers in the system are listed here.

Table 4-4 (Cont.) KPIs Server Elements

KPIs Status Element	Description
Server Indicators:	
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system.
RAM	Percentage utilization of physical memory on the server by all software as measured by TPD.
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.
Uptime	The total amount of time the server has been running.

Message Processor (MP) KPIs

The KPI values associated with **MP** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 4-5 MP KPIs

Variable	Description
Avg CPU Utilization	Percentage of CPU utilization by the Diameter process on a DA-**MP** server.
Offered Load (MPS)	Offered load on a DA-MP server, corresponding to the message rate before policing by capacity and congestion controls.
Accepted Load (MPS)	Accepted load on a DA-MP server, corresponding to the message rate after policing by capacity and congestion controls.
Messsage Processing Load (MPS)	Average message processing load (messages per second) on a MP server. The message processing load is the number of Diameter messages that are routed, including Reroute and MsgCopy.

Platform KPIs

The KPI values associated with **Platform** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 4-6 Platform KPIs

Variable	Description
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system.

Table 4-6 (Cont.) Platform KPIs

Variable	Description
RAM	Percentage utilization of physical memory on the server by all software as measured by TPD.
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.
Uptime	The total amount of time(days HH:MM:SS) the server has been running.

Process-based KPIs

Table 4-7 Process-based KPIs

Variable	Description
udr.Cpu	CPU usage of udr process
udr.MemBasTotal	Memory usage of the udr process
udr.MemPerTotal	Percent memory usage of udr process
udrbe.Cpu	CPU usage of udrbe process
udrbe.MemBasTotal	Memory usage of the udrbe process
udrbe.MemPerTotal	Percent memory usage of udrbe process
provimport.Cpu	CPU usage of provimport process
provimport.MemBasTotal	Memory usage of the provimport process
provimport.MemPerTotal	Percent memory usage of provimport process
provexport.Cpu	CPU usage of provexport process
provexport.MemBasTotal	Memory usage of the provexport process
provexport.MemPerTotal	Percent memory usage of provexport process
udrprov.Cpu	CPU usage of ras process
udrprov.MemBasTotal	Memory usage of the ras process
udrprov.MemPerTotal	Percent memory usage of ras process
udrprov.Cpu	CPU usage of xsas process
udrprov.MemBasTotal	Memory usage of the xsas process
udrprov.MemPerTotal	Percent memory usage of xsas process
era.Cpu	CPU usage of era process
era.MemBasTotal	Memory usage of the era process
era.MemPerTotal	Percent memory usage of era process

SS7/Sigtran KPIs

Table 4-8 SS7/Sigtran KPIs

Variable	Description
SCCP Recv Msgs/Sec	SCCP messages received per second.
SCCP Xmit Msgs/Sec	SCCP messages transmitted per second.
SS7 Process CPU Utilization	The average percent of SS7 Process CPU utilization on an MP server.
Ingress Message Rate	The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue.
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent.
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received.

UDRBE KPIs

Table 4-9 UDRBE KPIs

Variable	Description
RxAeProvCreateMsgsRate	Number of requests received via the provisioning interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber per second
RxAeProvCreateSubSuccessRate	Number of auto-enrolled subscribers created while provisioning non-profile entity data per second
RxAeShCreateSubSuccessRate	Number of auto-enrolled subscribers created via the Sh interface per second
RxAeShDeleteSubMsgs	Number of unsubscribe requests received via the Sh interface that triggered the removal of an auto-enrolled subscriber per second
RxAeShDeleteSubSuccess	Number of auto-enrolled subscribers deleted via the Sh interface per second
RxAeShPurCreateMsgsRate	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
RxAeShSnrCreateMsgsRate	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
RxPsoRequestRate	Number of inter-NO requests received per second

Table 4-9 (Cont.) UDRBE KPIs

Variable	Description
RxUdrBeReadMsgsRate	Number of read requests (across all interfaces) that have been received per second
RxUdrBeUpdateMsgsRate	Number of update requests (across all interfaces) that have been received per second
RxUdrNmNotifAckAsAvailableRate	Number of notification requests (across all interfaces) that have been successfully sent to the AS per second
RxUdrNmNotifAckAsUnavailableRate	Number of notification requests (across all interfaces) that failed to be sent to the AS per second
RxUdrSmSubscribeMsgsRate	Number of subscribe requests (across all interfaces) that have been received per second
RxUdrSmUnsubscribeMsgsRate	Number of unsubscribe requests (across all interfaces) that have been received per second
SQRQuotaRowElementsResetRate	Number of Quota Row Elements currently being reset or updated
SQRRecordsExaminedRate	Number of Subscriber/Pool Records currently being examined
SQRRecordsFailedRate	Number of Subscriber/Pool Records currently failed to reset or updated
SQRRecordsResetRate	Number of Subscriber/Pool Records currently being reset or updated
TxPsoRequestRate	Number of inter-NO requests sent per second
TxUdrBeReadReqSuccessRate	The number of read requests (across all interfaces) that have been successfully processed per second
TxUdrBeUpdateReqSuccessRate	The number of update requests (across all interfaces) that have been successfully processed per second
TxUdrNmNotifSentRate	The number of notification requests (across all interfaces) that have been sent per second
TxUdrSmSubscribeReqSuccessRate	The number of subscribe requests (across all interfaces) that have been successfully processed per second
TxUdrSmUnsubscribeReqSuccessRate	The number of unsubscribe requests (across all interfaces) that have been successfully processed per second

UDRFE KPIs

Table 4-10 **UDRFE *KPIs***

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

UDR RAS and XSAS Provisioning Related KPIs

Table 4-11 Provisioning KPIs

Variable	Description
ProvMsgsImportedRate	The number of provisioning messages imported per second
ProvTxnCommittedRate	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
RxRasDeleteReqReceivedRate	The number of REST DELETE requests that have been received on the provisioning interface per sec

Table 4-11 (Cont.) Provisioning KPIs

Variable	Description
RxRasGetReqReceivedRate	The number of REST GET requests that have been received on the provisioning interface per sec
RxRasPostReqReceivedRate	The number of REST POST requests that have been received on the provisioning interface per sec
RxRasProvConnection	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.
RxRasProvMsgsReceivedRate	The number of provisioning messages that have been received per second
RxRasProvMsgsSuccessfulRate	The number of provisioning messages that have been successfully processed per second
RxRasProvMsgsFailedRate	The number of provisioning messages that have failed to be processed due to errors per second
RxRasProvMsgsSentRate	The number of provisioning messages sent per second
RxRasProvMsgsDiscardedRate	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.
RxRasPutReqReceivedRate	The number of REST PUT requests that have been received on the provisioning interface per sec
RxRasResetReqReceivedRate	The number of REST Reset requests that have been received on the provisioning interface per sec
RxXsasDeleteReqReceivedRate	The number of SOAP delete requests that have been received on the provisioning interface per sec
RxXsasInsertReqReceivedRate	The number of SOAP insert requests that have been received on the provisioning interface per sec
RxXsasOperationReqReceivedRate	The number of SOAP operation requests that have been received on the provisioning interface per sec
RxXsasProvConnection	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.
RxXsasProvMsgsReceivedRate	The number of provisioning messages that have been received per second
RxXsasProvMsgsSuccessfulRate	The number of provisioning messages that have been successfully processed per second

Table 4-11 (Cont.) Provisioning KPIs

Variable	Description
RxXsasProvMsgsFailedRate	The number of provisioning messages that have failed to be processed due to errors per second
RxXsasProvMsgsSentRate	The number of provisioning messages sent per second
RxXsasProvMsgsDiscardedRate	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.
RxXsasProvTxnTotalRate	The number of provisioning SOAP transactions received per second
RxXsasResetReqReceivedRate	The number of SOAP Reset requests that have been received on the provisioning interface per sec
RxXsasSelectReqReceivedRate	The number of SOAP select requests that have been received on the provisioning interface per sec
RxXsasUpdateReqReceivedRate	The number of SOAP update requests that have been received on the provisioning interface per sec
TxProvTxnAbortedRate	The number of provisioning transactions that were aborted due to retry limit per second
TxProvTxnFailedRate	The number of provisioning transactions that have failed to be started or committed due to errors per second
TxProvTxnNonDurable	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
TxXsasProvTxnAbortedRate	The number of provisioning SOAP transactions that were aborted due to retry limit per second
TxXsasProvTxnFailedRate	The number of provisioning SOAP transactions that have failed to be started or committed, due to errors per second
XsasProvTxnCommittedRate	The number of provisioning SOAP transactions that have been successfully committed per second to the database

Ud Client KPIs

Table 4-12 Provisioning KPIs

Variable	Description
TxUdSearchRate	The number of LDAP search requests sent per second

Table 4-12 (Cont.) Provisioning KPIs

Variable	Description
TxUdSearchInitialRate	The number of LDAP search requests sent when initially creating a subscriber sent per second
TxUdSearchReSearchRate	The number of LDAP search requests sent when performing a re-search per second
TxUdSubscribeRate	The number of SOAP subscribe requests sent per second
TxUdSubscribeInitialRate	The number of SOAP subscribe requests sent when initially creating a subscriber sent per second sent per second
TxUdSubscribeReSubscribeRate	The number of SOAP subscribe requests sent when performing a re-subscribe per second
RxUdNotifyRate	The number of SOAP notify requests received per second
RxUdShUdrRate	The number of Sh UDR requests that trigger the Ud creation of a subscriber received per second
RxUdShPurRate	The number of Sh PUR requests that trigger the Ud creation of a subscriber received per second
RxUdShSnrRate	The number of Sh SNR requests that trigger the Ud creation of a subscriber received per second

5

Measurements

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 and measurement-related GUI elements.

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; for example, 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 (NOAM, 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 prefix in the Measurement tag. Prefixes include:

- **Alarm**: The measurement is associated with the severity or state of alarms.
- **CA**: The measurement is associated with the exceptions and unexpected messages and events that are specific to the Communication Agent protocol.
- **Conn**: The measurement is related to Diameter Connection congestion states.
- **DAS**: This is a Diameter Application Server measurement that reflects the Message Copy performance.
- **EV**: The measurement is associated with a link timing out when waiting for an ASP-ACTIVE acknowledgment message to be received.
- **Routing**: The measurement is associated with messages processed by the Diameter Routing Layer (**DRL**).
- **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.
- **SCTP**: The measurement is associated with the SCTP transport.
- **System**: The measurement is associated with the OAM system.
- **Tm**: The measurement is associated with the time aspect of message processing.
- **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.

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.

Application Routing Rules measurements

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

RxApplRuleSelected

Measurement ID
10085

Measurement Group
Application Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Application Routing Rule ID)

Description
Number of times that the application routing rule was selected for routing a Request message.

Collection Interval
5 min

Peg Condition
When DRL selects an application routing rule for routing a message.

Measurement Scope
Server Group

Recovery

1. No action required.

RxApplRuleFwdFailAll

Measurement ID
10086

Measurement Group
Application Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Application Routing Rule ID)

Description
Number of times that the application routing rule was selected for routing a Request message and the message was not successfully routed for any reason.

Collection Interval
5 min

Peg Condition
When DRL selects an application routing rule to route a Request message and one of the following conditions is met:

- The DSR Application's Operational Status is "Unavailable".
- The DSR Application's Operational Status is not "Unavailable" but the attempt to enqueue the message to the DSR Application failed.

Measurement Scope
Server Group

Recovery

1. No action required.

RxApplRuleFwdFailUnavail

Measurement ID
10087

Measurement Group
Application Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Application Routing Rule ID)

Description
Number of times that the application routing rule was selected for routing a Request message and the message was not successfully routed because DSR Application's Operational Status was "Unavailable".

Collection Interval
5 min

Peg Condition
When DRL selects an application routing rule to route a Request message and the DSR Application's Operational Status is "Unavailable".

Measurement Scope
Server Group

Recovery

1. No action required.

RxApplRuleDuplicatePriority

Measurement ID
10088

Measurement Group
Application Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Application Routing Rule ID)

Description
Number of times that the application routing rule was selected for routing a message but another application routing rule had the same priority and was ignored.

Collection Interval
5 min

Peg Condition
When DRL searches the ART and finds more than one highest priority application routing rule with the same priority that matches the search criteria. The measurement is associated with the application routing rule that is selected for routing.

Measurement Scope
Server Group

Recovery

1. Use GUI screen: **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules** to modify peer routing rule priorities.

   At least two application routing rules with the same priority matched an ingress Request message. The system selected the first application routing rule found. Application routing rules must be unique for the same type of messages to avoid unexpected routing results.

RxArtSelected

Measurement ID
10074

Measurement Group
Application Routing Rules

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of times that an application routing rule from ART-X was selected for routing a Request message

Collection Interval
5 min

Peg Condition
When DRL selects an application routing rule from ART-X for routing a message

Measurement Scope
Server Group

Recovery

1. No action required.

Association Exception measurements

The Association Exception measurement report contains measurements that provide information that is specific to associations configured for the MP server.

RxAsnFarEndClose

Measurement ID
9128

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
Number of times the far end closed the **SCTP** connection

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time the far-end of the association closes the association by sending either SHUTDOWN or ABORT.

Measurement Scope
NE, Server

Recovery

1. If the closing of the association was expected, no further action is necessary, the association will be recovered as soon as the far-end is ready to connect again. If the closing of the association was not expected. You can view Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.

2. Look in the event history from the GUI main menu under **Alarms & Events** > **View History** for Event ID 19224 to determine exactly when the far-end closed the association.
3. Look for other events for the association or MP server in the event history.
4. Verify that IP connectivity still exists between the MP server and the SG.
5. Verify whether the far-end of the association is undergoing maintenance.
6. It is recommended to contact My Oracle Support for assistance if needed.

EvAsnManClose

Measurement ID
9129

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of times the association was manually closed. This includes manual changes of the association administrative state that cause the association to transition from ASP-UP to either ASP-DOWN or **Disabled**.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time a manual change is made to the association administrative state from **Enabled** to **Blocked** or from **Enabled** to **Disabled**, causing the association to transition out of ASP-UP protocol state.

Measurement Scope
NE, Server

Recovery

1. If the association is known to be under maintenance no further action is necessary. If the association was not known to be under maintenance, you can view the Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. View the event history from the GUI main menu under **Alarms & Events** > **View History** and look for Event ID 19228. Event ID 19228 shows the manual association state transitions and contains a time-stamp of when the change occurred.
3. View the security logs from the GUI main menu under **Security** > **Logs**. You can search the logs using the time-stamp from the event history log to determine which login performed the manual state change on the association.

4. It is recommended to contact My Oracle Support for assistance if needed.

EvAsnNoRespClose

Measurement ID
9130

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension

Description
The number of times the association was closed due to lack of response from the far end. This includes lack of response to any signaling sent on the association or to SCTP heartbeating if enabled.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an established SCTP association is closed by the MP server due to lack of response at the SCTP level from the far-end of the association.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. If it has a non-zero value, the association has been closed due to the lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the Signaling Gateway. You can view the Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. Look in the event history from the GUI main menu under **Alarms & Events** > **View History** for Event ID 19225.
3. Verify IP connectivity between the MP server and the Signaling Gateway.
4. Determine if the far-end of the association is congested, possibly causing slow response times on the association.
5. Check the IP network between the MP server and the Signaling Gateway for excessive retransmissions.
6. It is recommended to contact My Oracle Support for assistance if needed.

EvTrCnxFail

Measurement ID
9404

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the SCTP connection attempt failed on the association. This includes only unsuccessful attempts to connect to the Signaling Gateway. It does not include failure of established connections.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an SCTP connect attempt fails.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Signaling Gateway at least once and failed to establish the SCTP connection.You can view Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. Check the event history log from the GUI main menu under **Alarms & Events** > **View History**, looking for Event ID 19222. Event ID 19222 provides details about the cause of the failure.
3. Verify that the Adjacent server that represents the far-end of the association is configured with the correct IP address. You can view the Adjacent servers from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Adjacent Servers**.
4. Verify that the remote port configured for the association correctly identifies the port that the Signaling Gateway is listening on for SCTP connections. You can view the configured port from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Associations** > **Configure**.
5. Verify the IP network connectivity between the MP server and the Signaling Gateway.
6. If the Signaling Gateway must be configured to connect to the MP server's IP address and port, verify that the signaling gateway configuration matches the association configuration. You can view association data from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Associations** > **Configure**.
7. It is recommended to contact My Oracle Support for assistance if needed.

TxAsnSendFail

Measurement ID
9133

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of times the SCTP Send failed for non-DATA M3UA signaling on the association. The number includes the sending of any non-DATA messages on an established association.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an attempt to send M3UA signaling fails for any reason and the information being sent cannot be mapped to a specific link

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this association using SCTP has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association. You can view Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. Look in the GUI main menu under **Alarms & Events** > **View History** in the event history log for Event ID 19233 - Failed to send non-DATA message. Refer to the *DSR Alarms and KPIs Reference* for details about this event and the cause of the failure to send.
3. Verify that the IP network between the MP server and the SG is functioning as expected.
4. It is recommended to contact My Oracle Support for assistance if needed.

RxAsnRecvFailed

Measurement ID
9134

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed. You can view Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. Look in the event history log from the GUI main menu under **Alarms & Events** > **View History** for Event ID 19223. Event ID 19223 gives more information about what caused the failure.
3. Try to bring the sockets back into alignment by manually **Disabling** and **Enabling** the association.
4. It is recommended to contact My Oracle Support for assistance if needed.

EvTrSockInitFail

Measurement ID
9407

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the socket initialization failed. Socket initialization includes configuring the association according to the settings in the GUI under **SS7/Sigtran** > **Configuration** > **Associations** > **Configuration Sets**.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time one or more socket options cannot be set according to the settings in the association's configuration set.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. A non-zero value indicates a problem with the association setup prior to attempting to connect the association. If this occurs, look for Event ID 19221 in the GUI under **Alarms & Events** > **View History**. Event 19221 provides details about the configuration failure.
2. It is recommended to contact My Oracle Support for further assistance.

RxAsnM3uaERROR

Measurement ID
9140

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of M3UA ERROR messages received on the association. An M3UA ERROR message is sent by the far-end to complain about an invalid M3UA message that it received.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA ERROR message is received that cannot be mapped to a specific link.

Measurement Scope
NE, Server

Recovery

1. This measurement will have a value of zero. A non-zero value indicates a problem with M3UA signaling sent by the MP server.
2. Look for Event ID 19235 from the GUI main menu under **Alarms & Events** > **View History**. Event ID19235 provides more information about the receipt of the ERROR message.
3. If the ERROR reason in Event ID 19235 indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. It is recommended to contact My Oracle Support for assistance if needed.

EvAsnUpAckTO

Measurement ID
9141

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of times the association timed out waiting for ASP-UP-ACK. ASP-UP-ACK is sent by the far-end in response to an ASP-UP message during the association start-up (when the association is in the **Enabled** administrative state).

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an ASP-UP has been sent and the M3UA State Management ACK Timer expires, but no ASP-UP-ACK has been received for the association.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. If the value is not zero, the association cannot be brought into the state necessary for M3UA ASPTM traffic because the far-end of the association is not responding by sending an ASP-UP-ACK prior to the timeout defined in the GUI under **SS7/Sigtran** > **Configuration** > **Options** > **M3UA**. The field that defines the timeout is the **State Management ACK Timer**.
2. You can view Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
3. Check the event history from the GUI main menu under **Alarms & Events** > **View History**, looking for Event ID 19226. Event ID 19226 will show when the timeout occurred.
4. Verify that the far-end of the association on the SG is not undergoing maintenance.
5. Verify that the **State Management ACK Timer** value is not set too short. This should not occur if the IP network is functioning correctly.
6. Verify that the IP network between the MP server and the SG is performing up to expectations.
7. It is recommended to contact My Oracle Support for assistance if needed.

RxAsnUnsolDownAck

Measurement ID
9142

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of unsolicited M3UA **ASP-DOWN-ACK** messages received on the association. Unsolicited **ASP**-DOWN-**ACK** messages can be sent by the **SG** to indicate that the SG cannot process traffic on the association.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an unsolicited ASP-DOWN-ACK is received on the association.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. A non-zero value means that the far-end of the association has stopped processing M3UA signaling. You can view Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. Check the event history from the GUI main menu under **Alarms & Events** > **View History**, looking for Event ID 19227. **Event ID 19227** will show exactly when the unsolicited ASP-DOWN-ACK was received.
3. Verify whether the far-end of the association is undergoing maintenance.
4. It is recommended to contact My Oracle Support for assistance if needed.

RxAsnInvalidM3ua

Measurement ID
9143

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number invalid M3UA messages received on this association. An invalid M3UA message is a message that violates the M3UA protocol.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA message is received on the association that is invalid due to any syntactic or semantic reason.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. In case of a non-zero value in this measurement, review the event history from the GUI main menu under **Alarms & Events** > **View History**, looking for Event 19231.
2. Event 19231 provides details about the reason for rejecting the M3UA message. If the error reason indicates a problem with routing context, verify that the routing context used for the association specified in Event 19231 is configured to match between the ASP and the SG.
3. It is recommended to contact My Oracle Support for assistance if needed.

TmSingleTransQueueFull

Measurement ID
9415

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of egress messages that were discarded because the single Transport Writer Queue was full.

Collection Interval
30 min

Peg Condition
Check whether the single peers transmit data queue limit has reached its max limit (1000). If maximum limit is reached or exceeded, then peg the measurement and discard the low priority events.

Measurement Scope
NE, Server

Recovery

1. This measurement indicates that the Transport is backed up and messages might be discarded. If the value is above the defined critical threshold, an alarm (19408) is generated. If the problem persists, it is recommended to contact My Oracle Support.

EvSctpAdjPToDwn

Measurement ID
9424

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
Number of times configured IP Address of an Adjacent Node goes from Available to Unavailable.

Collection Interval
30 min

Peg Condition
This measurement shall be incremented by one each time reachability to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected. If all is well, the measurement will have a zero value. A non-zero value indicates that a path fault to that address was detected.

Measurement Scope
NE, Server

Recovery

1. Check the event history log at **Main Menu** > **Alarms & Events** > **View History**; look for event ID 19410. Event ID 19410 provides more details about the actual cause of the failure.
2. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**.
3. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
4. If the problem persists, it is recommended to contact My Oracle Support.

EvSctpTransRej

Measurement ID
9425

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
Number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.

Collection Interval
30 min

Peg Condition
This measurement shall be incremented by one each time the association has been rejected due to IP address validation in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node. If all is well, the measurement has a zero value. A non-zero value indicates that an Adjacent Node has attempted to connect to the Peer IP Address at least once, but the connection attempt was rejected because the IP address advertised by the Adjacent Node failed validation.

Measurement Scope
NE, Server

Recovery

1. Check the Transport history at **Main Menu** > **Transport Manager** > **Maintenance**.
2. Verify IP network connectivity between the MP server and the Adjacent Nodes IP address using a ping or traceroute command.
3. Verify that the SCTP validation mode is the one that is needed.
4. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**.
5. Verify that the remote port configured at **Main Menu** > **Transport Manager** > **Configuration** > **Transport** for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.
6. If the problem persists, it is recommended to contact My Oracle Support.

Association Performance measurements

TxTrOctets

Measurement ID
9408

Measurement Group
Association Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of octets sent on the association. This includes **octets** for both DATA and non-DATA M3UA signaling. It does not include SCTP, **IP**, or **Ethernet** headers.

Collection Interval
30 min

Peg Condition
This measurement is incremented by the number of octets in the message each time a DATA/non-DATA message is successfully sent on the transport.

Measurement Scope
NE, **Server**

Recovery

1. No action required.

RxTrOctets

Measurement ID
9409

Measurement Group
Association Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of octets received on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers.

Collection Interval
30 min

Peg Condition
This measurement shall be incremented by the number of octets in the message each time a DATA/non-DATA message is successfully received on the transport.

Measurement Scope
NE, Server

Recovery

1. No action required.

SCTPAssocQueuePeak

Measurement ID
9169

Measurement Group
Association Performance

Measurement Type
Max

Measurement Dimension
Arrayed

Description
The peak SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.

Collection Interval
30 min

Peg Condition
Transport's queue is registered as a Stack Resource. The StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport.

Measurement Scope
NE, Server

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.
3. See Alarm 19408 - Single Transport Egress-Queue Utilization (refer to the *DSR Alarms and KPIs Reference* for details about this alarm).
4. It is recommended to contact My Oracle Support for assistance if needed.

SCTPAssocQueueAvg

Measurement ID
9170

Measurement Group
Association Performance

Measurement Type
Average

Measurement Dimension
Arrayed

Description
The average SCTP Single Association Writer Queue utilization (0-100%) measured during the collection interval.

Collection Interval
30 min

Peg Condition
The average of all SCTP Single Association Writer Queue utilization samples taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is a measure of how fast the Transport queue is processed and indicates the Average depth of queue over the monitored interval.
2. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
3. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum capacity of an MP over several collection intervals, then the number of MPs in the Network Element might need to be increased.
4. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element, then a MP-specific hardware, software, or configuration problem might exist.
5. If the problem persists, it is recommended to contact My Oracle Support.

Association Usage measurements

EvAsnCnxSuccess

Measurement ID
9131

Measurement Group
Association Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per association)

Description
The number of times the SCTP connection was successfully established on the association.

Collection Interval
30 min

Peg Condition
This measurement shall be incremented by one each time the SCTP association reaches the ASP-DOWN protocol state (for example, the connection is successfully established).

Measurement Scope
NE, Server

Recovery

1. If the association is expected to have connected during the measurement reporting interval, no action is necessary. Otherwise, preform the following steps:
2. You can view the transport status can be viewed from the GUI main menu under **Transport Manager** > **Maintenance** > **Transport**.
3. Look in the event history from the GUI main menu under **Alarms & Events** > **View History**. Look for events related to the association or the MP server to determine what might have caused the association to fail.
4. It is recommended to contact My Oracle Support for assistance if needed.

TmAsnBlkNotDown

Measurement ID
9138

Measurement Group
Association Usage

Measurement Type
Duration

Measurement Dimension
Arrayed (per association)

Description
The number of seconds during the reporting interval during which the association was in the **Blocked** administrative state but was not in ASP-DOWN state. When the association is **Blocked**, the desired protocol state is ASP-DOWN. This measurement

indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.

Collection Interval
30 min

Peg Condition
Time is accumulated for this measurement during the collection interval when all of the following are true:

- The association is in the **Blocked** administrative state.
- The association is not in the ASP-DOWN protocol state.

Measurement Scope
NE, Server

Recovery

1. The value of this measurement should be zero. A non-zero value indicates that the association was set to the **Blocked** administrative state, but was not able to reach the desired protocol state due to some problem. You can view the Association status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Associations**.
2. Verify the Adjacent server that represents the far-end of the association is configured with the correct IP address. You can check the configuration from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Adjacent Servers**.
3. Verify he remote port configured for the association correctly identifies the port that the SG is listening on for SCTP connections. You can check the configuration from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Associations** > **Configure**.
4. Verify the IP network connectivity between the MP server and the SG.
5. If the SG must be configured to connect to the MP server's IP address and port, verify that the SG configuration matches the association configuration. You can check the configuration from the GUI main menu under **SS7/Sigtran** > **Configuration** > **Associations** > **Configure**.
6. It is recommended to contact My Oracle Support for assistance if needed.

TmAsnEnaNotUp

Measurement ID
9139

Measurement Group
Association Usage

Measurement Type
Duration

Measurement Dimension
Arrayed (per association)

Description
The time that the association was enabled, but not in the ASP-UP state

Collection Interval
30 min

Peg Condition
Time shall be accumulated for this measurement during the collection interval when all of the following are true:

- the association is in the Enabled administrative state
- the association is not in the ASP-UP protocol state for any reason

Measurement Scope
NE, Server

Recovery

1. No action is required.

Communication Agent (ComAgent) Exception measurements

The **Communication Agent** Exception measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the **Communication Agent** protocol.

CADataFIFOQueueFul

Measurement ID
9971

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
StackEvents discarded due to ComAgent DataFIFO queue full condition. This value provides a measure of how many messages are discarded by ComAgent due to ComAgent User Data FIFO Queue full condition.

Collection Interval
30 min

Peg Condition
For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent User Data FIFO queue.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to contact My Oracle Support for assistance.

CADSTxDscrdCong

Measurement ID
9841

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of egress stack events discarded because the congestion level of the connection exceeded the stack events' priority level.

Collection Interval
30 min

Peg Condition
When **ComAgent** receives a stack event from a local User Layer to be transferred via the direct service and the selected connection has a congestion level greater than the priority level of the stack event.

Measurement Scope
Server

Recovery

1. When this measurement is increasing, it is an indication that the product is experiencing overload. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if the offered load is expected and exceeds the product's capacity.

   If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.

2. It is recommended to contact My Oracle Support for assistance.

CAHSRsrcErr

Measurement ID
9875

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of times that **ComAgent** receives in a heartbeat stack event status concerning a known Resource but an unknown Sub-Resource.

Collection Interval
30 min

Peg Condition
When **ComAgent** stores an unexpected Sub-Resource entry in the local Resource Provider Table. An unexpected Sub-Resource involves a known Resource but an unknown Sub-Resource ID (SRID). This condition is associated with Alarm-ID 19848, and only the first instance of an unexpected Sub-Resource is counted, not the repeats caused by multiple unknown Sub-Resources and the periodic heartbeats containing the same information.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** to determine configuration problems.
2. It is recommended to contact My Oracle Support for assistance.

CAHSTxDscrdCongSR

Measurement ID
9872

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of stack events discarded due to HA Service Sub-Resource congestion. During normal operation, this measurement should not be increasing. When this measurement is increasing, it is an indication that the product is experiencing overload.

Collection Interval
30 min

Peg Condition
Stack event submitted to **ComAgent** by a local User Layer, and the stack event references an HA Service Sub-Resource that has a congestion level greater than the priority level of the stack event.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if the offered load is expected and exceeds the product's capacity.

   If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur. If the load does not exceed the pproduct's capacity, then check the status of the servers hosting the Resource Providers to trouble-shoot the cause of the overload.

   This measurement may not indicate an error if the discarded stack event was a reliable request, the Reliable Transfer Function was able to re-attempt, and the subsequent attempt got through.

2. It is recommended to contact My Oracle Support for assistance.

CAHSTxDscrdIntErrSR

Measurement ID
9874

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.

Collection Interval
30 min

Peg Condition
User Layer submits to ComAgent an egress stack event destined to a known Sub-Resource and that is discarded due to a ComAgent internal error

Measurement Scope
Server

Recovery

1. Check other ComAgent measurements, alarms, and events to determine the source of the abnormality causing this measurement to arise.
2. If the problem persists, it is recommended to contact My Oracle Support.

CAHSTxDscrdUnavailSR

Measurement ID
9871

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of stack events discarded because they were submitted to an Unavailable Sub-Resource of a given Resource. During normal operation, this measurement should not be increasing. Each count of this measurement indicates that a local application attempted to send a stack event to another server using an HA Service Sub-Resource, but the event was discarded due to the Sub-Resource being unavailable.

Collection Interval
30 min

Peg Condition
Stack event submitted to **ComAgent** by a local User Layer, and the stack event references an Unavailable Sub-Resource.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to diagnose the cause of routing failures.

   If a discarded stack event was a request from a reliable transaction and the routing failure was due to a temporary condition, then it is possible that the transaction completed successfully using one or more retransmit attempts.

This measurement may not indicate an error if the discarded stack event was a reliable request, the Reliable Transfer Function was able to re-attempt, and the subsequent attempt got through.

2. It is recommended to contact My Oracle Support for assistance.

CAHSTxDscrdUnknownSR

Measurement ID
9870

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of egress stack events discarded because they referred to a known Resource and an unknown Sub-Resource. During normal operation this measurement should be 0. A non-zero value for this measurement indicates that **ComAgent** is improperly configured to support a local application.

Collection Interval
30 min

Peg Condition
User Layer submits to **ComAgent** an egress stack event that refers to an unknown Sub-Resource.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to verify that all HA Service Sub-Resources expected by local applications are present and operating.

2. It is recommended to contact My Oracle Support for assistance.

CAHSTxDscrdUnkwnRsrc

Measurement ID
9873

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of egress stack events discarded because they referred to an unknown Resource.

Collection Interval
30 min

Peg Condition
User Layer submits to **ComAgent** an egress stack event that refers to an unknown Resource.

Measurement Scope
Server

Recovery

1.

2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to verify that all HA Service Sub-Resources expected by local applications are present and operating.

3. It is recommended to contact My Oracle Support for assistance.

CAHSTxRsrc

Measurement ID
9876

Measurement Group
ComAgent Performance, **ComAgent** Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of egress stack events that were routed to a known Resource.

Collection Interval
30 min

Peg Condition
User Layer submits to **ComAgent** an egress stack event destined to a known Resource.

Measurement Scope
Server

Recovery

1. No action required.

CAMxFIFOQueueFul

Measurement ID
9970

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
StackEvents discarded due to ComAgent MxFIFO queue full condition. This value provides a measure of how many messages are discarded by ComAgent due to ComAgent internal connection MxFIFO Queue full condition.

Collection Interval
30 min

Peg Condition
For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent internal connection MxFIFO queue.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to contact My Oracle Support for assistance.

CAPSTxDscrdUnkwnGrp

Measurement ID
8013

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of egress stack events discarded because they referred to a Peer Group which was unknown

Collection Interval
30 min

Peg Condition
For each stack event submitted to ComAgent by a local User Layer and the stack event reference an Unknown Peer Group

Measurement Scope
Server

Recovery

1. A non-zero value of this measurement indicates that a local User Layer is malfunctioning and is attempting to use a Peer Group which it has not configured.
2. It is recommended to contact My Oracle Support for assistance.

CAPSTxDscrdUnavailGrp

Measurement ID
8014

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Group ID)

Description
The number of egress stack events discarded because they referred to a Peer Group which was unavailable

Collection Interval
30 min

Peg Condition
For each stack event submitted to ComAgent by a local User Layer and the stack event reference an Unavailable Peer Group

Measurement Scope
Server

Recovery

1. Each count of this measurement indicates that a local User Layer attempted to send a stack event to a remote server using ComAgent Peer Group Service, but the event was discarded due to the specified Peer Group being unavailable. The Peer Group may become unavailable due to:

   - Local User Layer performed maintenance action on the Peer Group that result in a loss of communication between servers.
   - Network problems that result in a loss of communication between servers.

2. It is recommended to contact My Oracle Support for assistance.

CAPSTxDscrdCongPeer

Measurement ID
8017

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Group ID)

Description
The number of egress stack events discarded because of Peer congestion.

Collection Interval
30 min

Peg Condition
For each stack event submitted to ComAgent by a local User Layer and the active Peer in the Peer Group has a congestion level greater than the priority level of the stack event.

Measurement Scope
Server

Recovery

1. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screens to determine if the offered load is expected and exceeds the product's capacity.

   If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.

2. It is recommended to contact My Oracle Support for assistance.

CARsrcPoolFul

Measurement ID
9859

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
ComAgent internal resource pool exhaustion condition.

Collection Interval
30 min

Peg Condition
This is to track the measure of the internal resource (Ex: CommMessage Resource pool) exhaustion condition for a given interval. For each resource allocation/access attempt that result in resource pool manager returning an indication that the maximum resources reserved are allocated and are in-use. When this condition occurs **ComAgent** tries to allocate a new resource from heap and relists it after its life cycle (Ex: CommMessage objects required for user data traffic for MxEndpoint interface).

Measurement Scope
NE, Server

Recovery

1. This value provides a measure of how many times pre-allocated resources are exhausted in **ComAgent** interfaces.

   This measurement is primarily intended for performance analysis and to assist in evaluating the need for any additional engineering processing capacity or tuning.

CARSTxDscrdCong

Measurement ID
9843

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of stack events discarded due to Routed Service congestion.

Collection Interval
30 min

Peg Condition
Stack event submitted to **ComAgent** by a local User Layer, and the stack event references a Routed Service that has a congestion level greater than the priority level of the stack event.

Measurement Scope
Server

Recovery

1. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screens to determine if the offered load is expected and exceeds the product's capacity.

   If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.

2. It is recommended to contact My Oracle Support for assistance.

CARSTxDscrdInternalErr

Measurement ID
9867

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of egress events discarded because of another Routed Service internal error

Collection Interval
30 min

Peg Condition
Each time an egress event is discarded because of another Router Service internal error

Measurement Scope
Server

Recovery

1. It is recommended to contact My Oracle Support for assistance.

CARSTxDscrdSvcUnavail

Measurement ID
9830

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of stack events discarded because they were submitted to an Unavailable Routed Service.

Collection Interval
30 min

Peg Condition
Stack event submitted to **ComAgent** by a local User Layer, and the stack event references an Unavailable Routed Service.

Note: Each count of this measurement indicates that a local application attempted to send a stack event to another server using a Routed Service, but the event was discarded due to the Routed Service being unavailable. Routing failures can occur due to:

- Maintenance actions are performed that result in a loss of communication between servers.
- Network problems result in a loss of communication between servers.
- Server overload can result in routes becoming unavailable for some stack events.

Measurement Scope
Server

Recovery

1. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screens to further diagnose the cause of routing failures.

   If a discarded stack event was a request from a reliable transaction and the routing failure was due to a temporary condition, then it is possible that the transaction completed successfully using one or more retransmit attempts.

2. It is recommended to contact My Oracle Support for assistance.

CARxDiscUnexpEvent

Measurement ID
9826

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded because it was unexpected in the connection operational state

Collection Interval
30 min

Peg Condition
For each ingress StackEvent that is discarded by **ComAgent** Stack, due to StackEvent received in unexpected connection state.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **ComAgent** due to message received in unexpected connection state.

CARxDscrdBundle

Measurement ID
9994

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress bundled event discarded during routing.

Collection Interval
30 min

Peg Condition
Each time an ingress bundled event is discarded during routing

Measurement Scope
Site

Recovery

1. No action required

CARxDscrdConnUnavail

Measurement ID

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension

Description
Number of User Data ingress events discarded because connection was not in-service.

Collection Interval
30 min

Peg Condition
For each User Data ingress StackEvent received from configured service peer server with connection status not “in-service”.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data ingress messages are discarded by **ComAgent** for the data messages received in connection not in “in-service” state.

CARxDscrdDecodeFailed

Measurement ID
9810

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded because failed to deserialize (event not part of stack service language).

Collection Interval
30 min

Peg Condition
For each StackEvent received from a configured peer server that resulted in any decode failures within **ComAgent** Stack.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **ComAgent** due to internal decode error condition.

CARxDscrdIncompat

Measurement ID
9825

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded because an Incompatible header version is received.

Collection Interval
30 min

Peg Condition
For each ingress StackEvent that is discarded by **ComAgent** Stack, due to unsupported base header version, as indicated in StackEvent.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **ComAgent** due to incompatible base header version of base software event library.

CARxDscrdInternalErr

Measurement ID
9818

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded because of other unexpected internal processing error.

Collection Interval
30 min

Peg Condition
For each ingress StackEvent that is discarded by **ComAgent** Stack, due to internal processing errors for conditions not covered by other meas-pegs.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **ComAgent** due to internal software processing errors for conditions not covered by other measurement pegs.

CARxDscrdLayerSendFail

Measurement ID
9812

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data ingress events discarded because layer's sendTo failed.

Collection Interval
30 min

Peg Condition
For each User Data StackEvent received from a configured service peer server and resulted in send failure to the destination stack layer.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data ingress messages are discarded by **ComAgent** due to internal send failure to destination stack layer.

CARxDscrdMsgLenErr

Measurement ID
9808

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded as it doesn't contain enough bytes (less than event header bytes).

Collection Interval
30 min

Peg Condition
For each StackEvent received from configured peer with message size less than the minimum required Header.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **Communication Agent** due to message size error.

CARxDscrdUnkServer

Measurement ID
9820

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded because the origination server was unknown/not configured.

Collection Interval
30 min

Peg Condition
For each ingress StackEvent that is discarded by **ComAgent** Stack, due to unknown origination IP address contents in StackEvent.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **ComAgent** due to unknown origination IP address in StackEvent.

CARxDscrdUnkStkLyr

Measurement ID
9811

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data ingress events discarded because stack layer is not known.

Collection Interval
30 min

Peg Condition
For each User Data ingress StackEvent received by **Communication Agent** Stack, for an unknown destination stack.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **Communication Agent** , as the destination stack is not registered/known.

CARxMsgUnknown

Measurement ID
9809

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ingress events discarded because stack event was unknown.

Collection Interval
30 min

Peg Condition
For each undefined StackEvent received from one of the configured peer server.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many ingress messages are discarded by **ComAgent** as the message is not defined/known to **ComAgent** Stack.

CAStackQueueFul

Measurement ID
9829

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed

Description
StackEvents discarded due to **ComAgent** task queue full condition.

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent that is discarded by **ComAgent** Stack, due to failure in attempting to put the messages in **ComAgent** Egress Task Queue.

Measurement Scope
NE, Server

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance.

CATransDscrdInvCorrId

Measurement ID
9832

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of received stack events that were received and discarded because they did not correlate with a pending transaction.

Collection Interval
30 min

Peg Condition
ComAgent receives a response stack event that contains a correlation ID that does not match a pending transaction record.

Measurement Scope
Server

Recovery

1. This measurement indicates that one or more destination servers are either responding to requests after a transaction has ended or are sending invalid responses. It is recommended to contact My Oracle Support for assistance.

CATransDscrdStaleErrRsp

Measurement ID
9833

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of times that an error response was discarded because it contained a valid correlation ID value but its originating server was not the last server to which the request was sent.

Collection Interval
30 min

Peg Condition
ComAgent receives an error response stack event that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent. This measurement indicates that one or more servers are responding with errors to requests after the local **ComAgent** has retransmitted the requests to other destination servers. This could occur due to:

- Network problems result in intermittent loss of communication between servers.
- Server overload results in delayed responses

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to check the status of the far-end servers and look for signs of overload.
2. It is recommended to contact My Oracle Support for assistance.

CATransEndAbnorm

Measurement ID
9834

Measurement Group
ComAgent Exception, **ComAgent** Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions that terminated abnormally.

Collection Interval
30 min

Peg Condition

- Transaction times-out waiting for a response, and the maximum number of transmits has been reached.
- Transaction time-to-live limit is exceeded.
- Transaction terminated due to lack of resources.

Note: This measurement is NOT pegged for these conditions:

- Transaction involves an unknown service.
- Transaction involves an unregistered Routed Service.

Measurement Scope
Server

Recovery

1. Check the **ComAgent** Exception report to further diagnose the reasons why transactions are failing.
2. It is recommended to contact My Oracle Support for assistance.

CATransEndAbnormRateAvg

Measurement ID
9865

Measurement Group
ComAgent Performance, **ComAgent** Exception

Measurement Type
Average

Measurement Dimension
Arrayed (by Service ID)

Description
Average rate per second that **ComAgent** transactions ended abnormally during the collection interval.

Collection Interval
30 min

Peg Condition
Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using a sliding-metric algorithm. The average transaction failure

rate is a running average, smoothed over approximately 10 seconds. This measurement provides the average rate per second that **ComAgent** transactions were started. This measurement is useful during troubleshooting when compared to other measurements.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransEndAbnormRateMax

Measurement ID
9866

Measurement Group
ComAgent Performance, **ComAgent** Exception

Measurement Type
Max

Measurement Dimension
Arrayed (by Service ID)

Description
Maximum rate per second that **ComAgent** transactions ended abnormally during the collection interval.

Collection Interval
30 min

Peg Condition
Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using a sliding-metric algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds. This measurement provides the maximum rate per second that **ComAgent** transactions were started. This measurement is useful during troubleshooting when compared to other measurements.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransEndAnsErr

Measurement ID
9845

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions initiated by local User Layers that ended with an error response from a destination server.

Collection Interval
30 min

Peg Condition
When a reliable response stack event (G=1, A=1, E=1) is received from a server to which a request was sent, and the response corresponds to a pending transaction record.

Measurement Scope
Server

Recovery

1. No action necessary.

   This measurement has value when compared against other measurements. Server applications may respond with errors as part of normal operations, as seen by **ComAgent**.

CATransEndErr

Measurement ID
9846

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions initiated by local User Layers that ended abnormally with an error response from a destination server.

Collection Interval
30 min

Peg Condition
When a valid reliable response stack event (G=1, A=0, E=1) is received from a server to which a request was sent, and the response corresponds to a pending transaction record. This measurement indicates that one or more destination servers are unable to process reliable requests received from the local server. This can be caused due to maintenance actions, server overload, and unexpected conditions in software.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support for assistance.

CATransEndNoResources

Measurement ID
9848

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions initiated by local User Layers that ended abnormally due to lack of resources.

Collection Interval
30 min

Peg Condition
ComAgent receives a reliable request (G=1, R=1) from a local User Layer and **ComAgent** is unable to allocate resources to process the transaction. This measurement indicates that the local server is exhausting its resources for processing reliable transactions. This can result when the combination of transaction rate and response delays exceeds engineered limits. High transaction rates can result from local server overload. Excess response delays can result from overloaded destination servers and problems in the network between servers.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support for assistance.

CATransEndNoResponse

Measurement ID
9847

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions initiated by local User Layers that ended abnormally due to a timeout waiting for a response.

Collection Interval
30 min

Peg Condition
Limit on the number of retransmits is reached with no response and limit on the transaction time-to-live is exceeded. This measurement indicates that one or more destination servers are unable to process reliable requests received from the local server. This can be caused due to maintenance actions, server overload, and unexpected conditions in software.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support for assistance.

CATransEndUnkwnSvc

Measurement ID
9842

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to an unknown service.

Collection Interval
30 min

Peg Condition
ComAgent receives a reliable request (G=1, R=1) from a local User Layer that refers to an unknown service. This measurement indicates improper configuration of **ComAgent** and/or a User Layer application.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Configuration** > **Routed Services** to confirm that all services expected by local applications are present.
2. It is recommended to contact My Oracle Support for assistance if needed.

CATransEndUnregSvc

Measurement ID
9861

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to a known service that lacked a registered User Layer.

Collection Interval
30 min

Peg Condition
ComAgent receives a reliable request (G=1, R=1) from a local User Layer that refers to a known service that has no registered User Layer.

Measurement Scope
Server

Recovery

1. A non-zero value in this measurement indicates a software malfunction. It is recommended to contact My Oracle Support for assistance.

CATransNoReTxMaxTTL

Measurement ID
9895

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions abnormally ended because of Max Time to live exceeded without any retransmits.

Collection Interval
30 min

Peg Condition
Maximum Time To Live period exceeded with no retransmission attempts and no response received for the transaction. This measurement provides a measure of abnormal transactions due to maximum time to live period exceeded condition (Without any retransmits) and no response is received from remote. Such abnormal transactions can be due to:

- Server overload that can result in delayed responses.
- Unexpected conditions in software.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support if assistance is needed

CATransRetx

Measurement ID
9831

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of times stack events were retransmitted.

Collection Interval
30 min

Peg Condition
ComAgent reliable transaction retransmit timer expires and the limit on the number of retransmits has not been reached. When this measurement is increasing, it indicates that communication between servers is experiencing unexpectedly high latency and/or packet loss. Retransmissions can occur due to:

- Maintenance actions are performed that result in a loss of communication between servers.
- Network problems result in a loss of communication between servers.
- Server overload can result in delayed responses.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support for assistance.

CATransReTxExceeded

Measurement ID
9894

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions abnormally ended because of Max number of Retries exceeded.

Collection Interval
30 min

Peg Condition
Number of retransmits limit is reached with no response received for the transaction. This measurement provides a measure of abnormal transactions due to maximum number of retransmission exceeded condition awaiting response from remote. Such abnormal transactions can be due to:

- Maintenance actions performed that result in a loss of communication between servers.
- Server overload that can result in delayed responses.

- Unexpected conditions in software.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support if assistance is needed

CATransStaleSuccessRsp

Measurement ID
9862

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of times that a success response was received from an unexpected server and was accepted to end a transaction.

Collection Interval
30 min

Peg Condition
ComAgent receives a success response stack event (G=1, A=1, E=1) that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent. This measurement indicates that a Routed Service received a success response from an unexpected server. This most commonly occurs if a server is slow to respond, **ComAgent** retransmits a request to another server, and then the original server finally responds to the request.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to diagnose stale responses.
2. It is recommended to contact My Oracle Support for assistance.

CATransTTLExceeded

Measurement ID
9893

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions abnormally ended because of Max Time to live exceeded.

Collection Interval
30 min

Peg Condition
Maximum Time To Live period exceeded with at least one retransmission attempted and no response received for the transaction. This measurement provides a measure of abnormal transactions due to maximum time to live period exceeded condition (Where at least one retransmission was also attempted) and no response is received from remote. Such abnormal transactions can be due to:

- Maintenance actions performed that result in a loss of communication between servers.
- Server overload that can result in delayed responses.
- Unexpected conditions in software.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine network and server communications.
2. It is recommended to contact My Oracle Support if assistance is needed

CATxDscrdBundle

Measurement ID
9993

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of egress bundled event discarded during routing.

Collection Interval
30 min

Peg Condition
Each time an egress bundled event is discarded during routing

Measurement Scope
Site

Recovery

1. No action required

CATxDscrdConnUnAvail

Measurement ID
9802

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events discarded because connection was not in-service(down/blocked/not aligned).

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent that is discarded by **ComAgent** Stack, due to connection status not being in-service.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data egress messages are discarded by **ComAgent** due to connection unavailability reasons.

CATxDscrdDestUserIncmpat

Measurement ID
9803

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events discarded because the remote doesn't support requested capabilities (either it doesn't support stack or event library or event library version is incompatible).

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent that is discarded by **Communication Agent** Stack, due to incompatibility in requested library id/version and the one known by **Communication Agent**.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data egress messages are discarded by **Communication Agent** due to remote not supporting requested capabilities.

CATxDscrdEncodeFail

Measurement ID
9804

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events discarded because of serialization failures.

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent that is discarded by **Communication Agent** Stack, due to any local encode failures.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data egress messages are discarded by **Communication Agent** due to local encode failure.

CATxDscrdInternalErr

Measurement ID
9817

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of egress events discarded because of other unexpected internal processing error.

Collection Interval
30 min

Peg Condition
For each egress StackEvent that is discarded by **ComAgent** Stack, due to internal processing errors for conditions not covered by other meas-pegs.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many egress messages are discarded by **ComAgent** due to internal software processing errors for conditions not covered by other measurement pegs.

CATxDscrdMxSendFail

Measurement ID
9805

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events discarded because of failure reported by MxEndpoint.

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent that is discarded by **Communication Agent** Stack, due to send failure as indicated by underlying transport.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data egress messages are discarded by **Communication Agent** due to transport reported error condition.

CATxDscrdUnknownSvc

Measurement ID
9849

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of non-reliable and non-request (G=0 or R=0) egress stack events discarded because they refer to an unknown service.This measurement indicates that **ComAgent** is improperly configured to support a local application.

Collection Interval
30 min

Peg Condition
User Layer submits to **ComAgent** a non-reliable or non-request (G=0 or R=0) egress stack event that refers to an unknown service.

Measurement Scope
Server

Recovery

1. Use **Main Menu** > **Communication Agent** > **Configuration** > **Routed Services** screen to verify that all Routed Services expected by local applications are properly configured.
2. It is recommended to contact My Oracle Support for assistance.

CATxDscrdUnkServer

Measurement ID
9819

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of egress events discarded because the destination server was unknown/not configured.

Collection Interval
30 min

Peg Condition
For each egress StackEvent that is discarded by **ComAgent** Stack, due to unknown destination IP address contents in StackEvent.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many egress messages are discarded by **ComAgent** due to unknown destination IP address in StackEvent.

CATxDscrdUnregSvc

Measurement ID
9860

Measurement Group
ComAgent Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of egress stack events discarded because they reference a known service that has no registered User Layer.

Collection Interval
30 min

Peg Condition
User Layer submits to **ComAgent** an egress stack event that refers to a known service that lacks a registered User Layer.

Measurement Scope
Server

Recovery

1. A non-zero measurement indicates that a local application is malfunctioning and is attempting to use a service for which it has not registered. It is recommended to contact My Oracle Support for assistance.

Communication Agent (ComAgent) Performance measurements

The **Communication Agent** Performance measurement group is a set of measurements that provide performance information that is specific to the **Communication Agent** protocol. These measurements will allow the user to determine how many messages are successfully forwarded and received to and from each DSR Application.

CAAvgDataFIFOQueueUtil

Measurement ID
9969

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed

Description
Average percentage of ComAgent DataFIFO Queue Utilization.

Collection Interval
30 min

Peg Condition
The average ComAgent connection DataFIFO Queue utilization sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating any issues with ComAgent User Data StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to contact My Oracle Support for assistance.

CAAvgMxFIFOQueueUtil

Measurement ID
9967

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed

Description
Average percentage of ComAgent MxFIFO Queue Utilization.

Collection Interval
30 min

Peg Condition
The average ComAgent connection MxFIFO Queue utilization sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating any issues with internal StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to contact My Oracle Support for assistance.

CAAvgQueueUtil

Measurement ID
9828

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed

Description
Average percentage of Queue Utilization.

Collection Interval
30 min

Peg Condition
The average **ComAgent** Egress Task Queue utilization sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance.

CAAvgRsrcPoolUtil

Measurement ID
9858

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Average percentage of internal resource pool utilization.

Collection Interval
30 min

Peg Condition
This is to track the measure of average usage of the internal resource (Ex: CommMessage Resource pool) for a given interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating the need for additional processing or performance capacity tuning on a node.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of a node over several collection intervals, then the internal engineering resource pool capacity or other dependent parameters may need to be tuned, so that it does not result in unaccounted latency.

CAAvgRxStackEvents

Measurement ID
9822

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Average Number of User Data ingress events received.

Collection Interval
30 min

Peg Condition
The average User Data ingress StackEvent sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. No action required.

This value provides a measure of Average Value during the interval, for number of User Data messages received from remote.

CAAvgTxStackEvents

Measurement ID
9816

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Single

Description
Average Number of User Data egress events received from stacks to deliver it to remote.

Collection Interval
30 min

Peg Condition
The average User Data egress StackEvent sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of Average Value during the interval, for number of User Data messages transmitted to remote.

CADSTx

Measurement ID
9814

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events specifically for the default Direct Service.

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent received specifically for the default Direct Service and processed by **ComAgent** Stack.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data egress messages are received by **ComAgent** to be transmitted from hosting server to destined remote server using default Direct "EventTransfer" Service.

CAHSTxRsrc

Measurement ID
9876

Measurement Group
ComAgent Performance, **ComAgent** Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Resource ID)

Description
Number of egress stack events that were routed to a known Resource.

Collection Interval
30 min

Peg Condition
User Layer submits to **ComAgent** an egress stack event destined to a known Resource.

Measurement Scope
Server

Recovery

1. No action required.

CAHSTxRsrcRateAvg

Measurement ID
9877

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Resource ID)

Description
Average rate per second of egress stack events routed to a known Resource.

Collection Interval
30 min

Peg Condition
Based upon the SysMetric.

Measurement Scope
Server

Recovery

1. No action required.

CAHSTxRsrcRateMax

Measurement ID
9878

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Resource ID)

Description
Maximum rate per second of egress stack events routed to a known Resource.

Collection Interval
30 min

Peg Condition
Based upon the SysMetric.

Measurement Scope
Server

Recovery

1. No action required.

CAPeakDataFIFOQueueUtil

Measurement ID
9968

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Arrayed

Description
Maximum percentage of ComAgent DataFIFO Queue Utilization.

Collection Interval
30 min

Peg Condition
The maximum ComAgent DataFIFO Queue utilization sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating any issues with ComAgent User Data StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to contact My Oracle Support for assistance.

CAPeakMxFIFOQueueUtil

Measurement ID
9966

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Arrayed

Description
Maximum percentage of ComAgent MxFIFO Queue Utilization.

Collection Interval
30 min

Peg Condition
The maximum ComAgent connection MxFIFO Queue utilization sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating any issues with internal StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

2. It is recommended to contact My Oracle Support for assistance.

CAPeakQueueUtil

Measurement ID
9827

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Arrayed

Description
Maximum percentage of Queue Utilization.

Collection Interval
30 min

Peg Condition
The maximum **ComAgent** Egress Task Queue utilization sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance.

CAPeakRsrcPoolUtil

Measurement ID
9857

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Maximum percentage of internal resource pool utilization.

Collection Interval
30 min

Peg Condition
This is to track the measure of maximum usage of the internal resource (Ex: CommMessage Resource pool) for a given interval.

Measurement Scope
NE, Server

Recovery

1. This measurement is primarily intended to assist in evaluating the need for additional processing or performance capacity tuning on a node.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of a node over several collection intervals, then the internal engineering resource pool capacity or other dependent parameters may need to be tuned, so that it does not result in unaccounted latency.

CAPeakRxStackEvents

Measurement ID
9821

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Maximum Number of User Data ingress events received.

Collection Interval
30 min

Peg Condition
The maximum User Data ingress StackEvent sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of Peak Value during the interval, for number of User Data messages received from remote.

CAPeakTxStackEvents

Measurement ID
9815

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Single

Description
Maximum Number of User Data egress events received from stacks to deliver it to remote.

Collection Interval
30 min

Peg Condition
The maximum User Data egress StackEvent sample taken during the collection interval.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of Peak Value during the interval, for number of User Data messages transmitted to remote.

CAPSTxGrp

Measurement ID
8015

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Group ID)

Description
The number of egress stack events submitted to the Peer Group Service to be routed to a known Peer Group.

Collection Interval
30 min

Peg Condition
For each stack event submitted to ComAgent Peer Group Service by a local User Layer

Measurement Scope
Server

Recovery

1. No action required. This measurement is useful when compared with other Peer Group Service measurements.

CAPSTxGrpSuccess

Measurement ID
8016

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Group ID)

Description
The number of egress stack events successfully routed to a known Peer Group.

Collection Interval
30 min

Peg Condition
For each stack event submitted to ComAgent Peer Group Service by a local User Layer and successfully routed

Measurement Scope
Server

Recovery

1. No action required. This measurement is useful when compared with other Peer Group Service measurements.

CARSTx

Measurement ID
9844

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of stack events submitted to a Routed Service for routing.

Collection Interval
30 min

Peg Condition
Stack event submitted to **ComAgent** Routed Service by a local User Layer

Measurement Scope
Server

Recovery

1. No action necessary

CARx

Measurement ID
9806

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data ingress events received from a peer server.

Collection Interval
30 min

Peg Condition
For each User Data StackEvent received from one of the configured peer and processed by **Communication Agent** Stack.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data ingress messages are received by **Communication Agent** to be transmitted to local hosting stack. This measurement count should be equal to the summation of User Data ingress events success and all User Data ingress events discards measurement counts

CARxBundled

Measurement ID
9986

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ComAgent Bundled events received by ComAgent

Collection Interval
30 min

Peg Condition
Each time a ComAgent Bundled event is received by ComAgent

Measurement Scope
Site

Recovery

1. No action required

CARxEventsBundled

Measurement ID
9988

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of stackevents received in ComAgent Bundled events

Collection Interval
30 min

Peg Condition
Each time a stackevent is received in ComAgent Bundled events

Measurement Scope
Site

Recovery

1. No action required

CARxSuccess

Measurement ID
9807

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data ingress events successfully routed to local layers.

Collection Interval
30 min

Peg Condition
For each User Data StackEvent received from a peer server and successfully transmitted to the local stack.

Measurement Scope
NE, Server

Recovery

1. No action required.

This value provides a measure of how many User Data ingress messages are received by **Communication Agent** and are successfully transmitted to local hosting stack.

CATransEndAbnorm

Measurement ID
9834

Measurement Group
ComAgent Exception, **ComAgent** Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions that terminated abnormally.

Collection Interval
30 min

Peg Condition

- Transaction times-out waiting for a response, and the maximum number of transmits has been reached.
- Transaction time-to-live limit is exceeded.
- Transaction terminated due to lack of resources.

Note: This measurement is NOT pegged for these conditions:

- Transaction involves an unknown service.
- Transaction involves an unregistered Routed Service.

Measurement Scope
Server

Recovery

1. Check the **ComAgent** Exception report to further diagnose the reasons why transactions are failing.
2. It is recommended to contact My Oracle Support for assistance.

CATransEndAbnormRateAvg

Measurement ID
9865

Measurement Group
ComAgent Performance, **ComAgent** Exception

Measurement Type
Average

Measurement Dimension
Arrayed (by Service ID)

Description
Average rate per second that **ComAgent** transactions ended abnormally during the collection interval.

Collection Interval
30 min

Peg Condition
Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using a sliding-metric algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds. This measurement provides the average rate per second that **ComAgent** transactions were started. This measurement is useful during troubleshooting when compared to other measurements.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransEndAbnormRateMax

Measurement ID
9866

Measurement Group
ComAgent Performance, **ComAgent** Exception

Measurement Type
Max

Measurement Dimension
Arrayed (by Service ID)

Description
Maximum rate per second that **ComAgent** transactions ended abnormally during the collection interval.

Collection Interval
30 min

Peg Condition
Rate of transaction failures due to final timeouts. Failed Transaction Rate monitoring is an average rate using a sliding-metric algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds. This

measurement provides the maximum rate per second that **ComAgent** transactions were started. This measurement is useful during troubleshooting when compared to other measurements.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransEndNorm

Measurement ID
9836

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions initiated by local User Layers that ended normally with a response from a destination server.

Collection Interval
30 min

Peg Condition
When a valid reliable response stack event (G=1, A=1) is received that corresponds to a pending transaction record.

Measurement Scope
Server

Recovery

1. No action necessary.

   This measurement has value when compared against other measurements. If no new transactions are started, then during normal operation, this measurement should match CATransStarted .

CATransPendingAvg

Measurement ID
9838

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Service ID)

Description
Average number of allocated pending transaction records over the collection interval.

Collection Interval
30 min

Peg Condition
Average number of allocated pending transaction records during the collection interval.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransPendingMax

Measurement ID
9837

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Service ID)

Description
Maximum number of allocated pending transaction records.

Collection Interval
30 min

Peg Condition
When a pending transaction record is allocated, and the total count of allocated pending transaction records exceeds the current peak.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransRateAvg

Measurement ID
9863

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Service ID)

Description
Average rate per second that **ComAgent** transactions were started during the collection interval.

Collection Interval
30 min

Peg Condition
Transaction rate monitoring is an average rate using a sliding-metric algorithm. The average transaction rate is a running average, smoothed over approximately 10 seconds. This measurement provides the average rate per second that **ComAgent** transactions were started. This measurement is useful during troubleshooting when compared to other measurements.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransRateMax

Measurement ID
9864

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Service ID)

Description
Maximum rate per second that **ComAgent** transactions were started during the collection interval.

Collection Interval
30 min

Peg Condition
Transaction rate monitoring is an average rate using a sliding-metric algorithm. The average transaction rate is a running average, smoothed over approximately 10 seconds. This measurement provides the maximum rate per second that **ComAgent** transactions were started. This measurement is useful during troubleshooting when compared to other measurements.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransStarted

Measurement ID
9835

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Service ID)

Description
Number of reliable transactions initiated by local User Layers.

Collection Interval
30 min

Peg Condition
When a valid reliable request stack event (G=1, R=1) is received from a local User Layer.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransTimeAvg

Measurement ID
9840

Measurement Group
ComAgent Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Service ID)

Description
Average transaction life-time in milliseconds.

Collection Interval
30 min

Peg Condition
Transaction ends either normally or abnormally.

Measurement Scope
Server

Recovery

1. No action necessary.

CATransTimeMax

Measurement ID
9839

Measurement Group
ComAgent Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Service ID)

Description
Maximum transaction life-time in milliseconds.

Collection Interval
30 min

Peg Condition
Transaction ends either normally or abnormally.

Measurement Scope
Server

Recovery

1. No action necessary.

CATx

Measurement ID
9800

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events received on **Communication Agent** task queue from local stacks to deliver it to a peer server.

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent received and processed by **Communication Agent** Stack.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data egress messages are received by **Communication Agent** for direct or indirect routing service.

   This measurement count should be equal to the summation of User Data egress events success and all User Data egress events discards measurement counts.

   This measurement count should be equal to the summation of User Data egress events received by **Communication Agent** for each (Direct, Routed and HA) routing service.

CATxBundled

Measurement ID
9985

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of ComAgent Bundled events transmitted by ComAgent

Collection Interval
30 min

Peg Condition
Each time a ComAgent Bundled event is transmitted by ComAgent

Measurement Scope
Site

Recovery

1. No action required

CATxEventsBundled

Measurement ID
9987

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of stackevents transmitted through ComAgent Bundled events

Collection Interval
30 min

Peg Condition
Each time a stackevent is transmitted through ComAgent Bundled events

Measurement Scope
Site

Recovery

1. No action required

CATxSuccess

Measurement ID
9801

Measurement Group
ComAgent Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of User Data egress events successfully delivered to a peer server.

Collection Interval
30 min

Peg Condition
For each User Data egress StackEvent transmitted to the peer server.

Measurement Scope
NE, Server

Recovery

1. No action required.

   This value provides a measure of how many User Data messages are successfully transmitted from hosting server to destined remote server over "event transfer" static connection.

Connection Congestion measurements

The Connection Congestion measurement report contains per-connection measurements related to Diameter Connection congestion states. Measurements in this group include:

- Congestion Level-X time duration
- Number of times entered Congestion Level-X
- Number of times Remote Busy Congestion occurred

RxRejectedConnCongestion

Measurement ID
10004

Measurement Group
Connection Congestion

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of Request messages from a downstream peer rejected by a Local Node because of Diameter Connection Congestion.

Collection Interval
5 min

Peg Condition
Each time an ingress transaction is abandoned and the Routing Option Set "Connection Congestion" action is invoked.

Measurement Scope
Site

Recovery

1. No action required.

Connection Exception measurements

The Connection Exception measurement report contains measurements that provide information about exceptions and unexpected messages and events for individual SCTP/TCP connections that are not specific to the Diameter protocol.

EvRxException

Measurement ID
18008

Measurement Group
Connection Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of connection ingress message processing exception events.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each EvRxException event, regardless of event reason or throttling.

Measurement Scope
Site

Recovery

1. No action required.

EvTxException

Measurement ID
18009

Measurement Group
Connection Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress message processing exception events.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each EvTxException event, regardless of event reason or throttling.

Measurement Scope
Site

Recovery

1. No action required.

Connection Performance measurements

The Connection Performance measurement report contains measurements that provide performance information for individual SCTP/TCP connections that are not specific to the Diameter protocol.

DclTxConnQueueAvg

Measurement ID
10224

Measurement Group
Connection Performance

Measurement Type
Average

Measurement Dimension
Arrayed (Connection ID)

Description
DCL egress connection message queue utilization average.

Collection Interval
5 min

Peg Condition
Output measurement of the DclTxConnQueue metric.

Measurement Scope
Site

Recovery

1. No action required.

DclTxConnQueuePeak

Measurement ID
10223

Measurement Group
Connection Performance

Measurement Type
Max

Measurement Dimension
Arrayed (Connection ID)

Description
DCL egress connection message queue utilization peak.

Collection Interval
5 min

Peg Condition
Output measurement of the DclTxConnQueue metric.

Measurement Scope
Site

Recovery

1. No action required.

EcCL1

Measurement ID
10524

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection onset for egress message rate in congestion level 1.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each onset of CL1.

Measurement Scope
Site

Recovery

1. No action required.

EcCL2

Measurement ID
10525

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection onset for egress message rate in congestion level 2.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each onset of CL2.

Measurement Scope
Site

Recovery

1. No action required.

EcCL3

Measurement ID
10526

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection onset for egress message rate in congestion level 3.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each onset of CL3.

Measurement Scope
Site

Recovery

1. No action required.

EcCL98

Measurement ID
10527

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection onset for egress message rate in congestion level 98.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each onset of CL98.

Measurement Scope
Site

Recovery

1. No action required.

EcRateAvg

Measurement ID
10193

Measurement Group
Connection Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress message rate average.

Collection Interval
5 min

Peg Condition
Output measurement of the EcRate metric.

Measurement Scope
Site

Recovery

1. No action required.

EcRatePeak

Measurement ID
10192

Measurement Group
Connection Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress message rate peak.

Collection Interval
5 min

Peg Condition
Output measurement of the EcRate metric.

Measurement Scope
Site

Recovery

1. No action required.

Ert

Measurement ID
18054

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress messages on routing egress.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message during the Egress Routing phase.

Measurement Scope
Site

Recovery

1. No action required.

ErtDrop

Measurement ID
18044

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of DA-MP egress messages discarded or rejected by routing egress.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message dropped during the Routing Egress phase.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvFsmOpState	StateChange (TransportCongestion)
	EvTxException	ConnUnavailable
DCL	EvTxException	DclTxConnQueueCongested
		DtlsMsgOversized
RCL	MpEvTxException	RclTxTaskQueueCongested
		EtrPoolCongested
		RadiusMsgPoolCongested
		SharedSecretUnavailable
		RadiusIdPoolCongested

Layer	Event	Reason
	EvTxException	MsgAttrLenUnsupported
		MsgTypeUnsupported
		MsgLenInvalid
		AnsOnClientConn
		ReqDuplicate

Measurement Scope
Site

Recovery

1. No action required.

Ic

Measurement ID
18053

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message during the Ingress Control phase.

Measurement Scope
Site

Recovery

1. No action required.

IcDrop

Measurement ID
18041

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages discarded or rejected by ingress control.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Ingress Control phase.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvRxException	MaxMpsExceeded

Measurement Scope
Site

Recovery

1. No action required.

IcDropP0

Measurement ID
18063

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress messages discarded or rejected by ingress control with priority 0.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Ingress Control phase with priority 0.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvRxException	MaxMpsExceeded

Measurement Scope
Site

Recovery

1. No action required.

IcDropP1

Measurement ID
18064

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress messages discarded or rejected by ingress control with priority 1.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Ingress Control phase with priority 1.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvRxException	MaxMpsExceeded

Measurement Scope
Site

Recovery

1. No action required.

IcDropP2

Measurement ID
18065

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress messages discarded or rejected by ingress control with priority 2.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Ingress Control phase with priority 2.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvRxException	MaxMpsExceeded

Measurement Scope
Site

Recovery

1. No action required.

IcDropP3

Measurement ID
18066

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress messages discarded or rejected by ingress control with priority 3.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Ingress Control phase with priority 3.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvRxException	MaxMpsExceeded

Measurement Scope
Site

Recovery

1. No action required.

IcRateAvg

Measurement ID
10500

Measurement Group
Connection Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress message rate average.

Collection Interval
5 min

Peg Condition
Output measurement of the IcRate metric.

Measurement Scope
Site

Recovery

1. No action required.

IcRatePeak

Measurement ID
10501

Measurement Group
Connection Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress message rate peak.

Collection Interval
5 min

Peg Condition
Output measurement of the IcRate metric.

Measurement Scope
Site

Recovery

1. No action required.

Irt

Measurement ID
18067

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress messages on routing ingress.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message during the Ingress Routing phase.

Measurement Scope
Site

Recovery

1. No action required.

IrtDrop

Measurement ID
18043

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages discarded or rejected by routing ingress.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Routing Ingress phase.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	MpEvRxException	DiamMsgPoolCongested
		SigEvPoolCongested
		DstMpUnknown
		DstMpCongested
		DrlReqQueueCongested
		DrlAnsQueueCongested
		ComAgentCongested
RCL	MpEvRxException	RadiusMsgPoolCongested
		RclRxTaskQueueCongested
		RclSigEvPoolCongested
		SharedSecretUnavailable
		ItrPoolCongested
	EvRxException	MsgAttrLenInvalid
		MsgAttrLenUnsupported
		AnsOrphaned
		AccessAuthMissing
		StatusAuthMissing
		MsgAuthInvalid
		ReqAuthInvalid
		AnsAuthInvalid
		MsgAttrAstUnsupported
		ReqDuplicate
		MsgTypeMissingMccs
		ConnUnavailable

Measurement Scope
Site

Recovery

1. No action required.

OcDrop

Measurement ID
18042

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages discarded or rejected by overload control.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Overload Control phase.
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	MpEvRxException	CpuCongested

Measurement Scope
Site

Recovery

1. No action required.

RadiusXactionFailAvg

Measurement ID
18234

Measurement Group
Connection Performance

Measurement Type
Average

Measurement Dimension
Single

Description
RADIUS connection transaction failure rate average.

Collection Interval
5 min

Peg Condition
The average RADIUS connection transaction failure rate sample taken during the collection interval.

Measurement Scope
Site

Recovery

1. No action required.

RxAll

Measurement ID
10104

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of connection ingress messages (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message during the Rx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

RxAllDrop

Measurement ID
10171

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages dropped (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message dropped during the Rx phase (routable and peer-to-peer).
The associated reasons can be found in this table:

Layer	Event	Reason
DCL	EvRxException	MsgInvalid
RCL	EvRxException	MsgTypeUnsupported

Measurement Scope
Site

Recovery

1. No action required.

RxAllLenAvg

Measurement ID
18036

Measurement Group
Connection Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress message length average (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is updated for each ingress message during the Rx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

RxAllLenPeak

Measurement ID
18037

Measurement Group
Connection Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress message length peak (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is updated for each ingress message during the Rx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

RxNgnPsAccepted

Measurement ID
18059

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress NGN-PS messages accepted.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress NGN-PS message accepted during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxNgnPsOffered

Measurement ID
18058

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress NGN-PS messages offered.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress NGN-PS message offered during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxP0

Measurement ID
18038

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages with priority 0.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message with priority 0 during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxP1

Measurement ID
18039

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages with priority 1.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message with priority 1 during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxP2

Measurement ID
18040

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages with priority 2.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message with priority 2 during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxP3

Measurement ID
10152

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages with priority 3.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message with priority 3 during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxP4

Measurement ID
18062

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress messages with priority 4.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message with priority 4 during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

RxSctpChunkMp

Measurement ID
10516

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of SCTP data chunks received by the MP (excluding duplicates).

Collection Interval
5 min

Peg Condition
SCTP statistics polling.

Measurement Scope
Server Group

Recovery

1. No action required.

RxSctpPacketMp

Measurement ID

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of SCTP packets received by the MP (excluding duplicates).

Collection Interval
5 min

Peg Condition
SCTP statistics polling.

Measurement Scope
Server Group

Recovery

1. No action required.

TmEcCL1

Measurement ID
10520

Measurement Group
Connection Performance

Measurement Type
Timer

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for egress message rate in congestion level 1.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is in CL1.

Measurement Scope
Site

Recovery

1. No action required.

TmEcCL2

Measurement ID
10521

Measurement Group
Connection Performance

Measurement Type
Timer

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for egress message rate in congestion level 2.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is in CL2.

Measurement Scope
Site

Recovery

1. No action required.

TmEcCL3

Measurement ID
10522

Measurement Group
Connection Performance

Measurement Type
Timer

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for egress message rate in congestion level 3.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is in CL3.

Measurement Scope
Site

Recovery

1. No action required.

TmEcCL98

Measurement ID
10523

Measurement Group
Connection Performance

Measurement Type
Timer

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for egress message rate in congestion level 98.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is in CL98.

Measurement Scope
Site

Recovery

1. No action required.

TxAll

Measurement ID
10100

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress messages (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message during the Tx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

TxAllDrop

Measurement ID
18050

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress messages dropped (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message dropped during the Tx phase (routable and peer-to-peer).
The associated reasons can be found in this table:

Layer	Event	Reason
CSL	EvFsmOpState	StateChange (TransportCongestion)
	EvTxException	ConnUnavailable
RCL	EvTxException	WriteFailure

Measurement Scope
Site

Recovery

1. No action required.

TxAllLenAvg

Measurement ID
18048

Measurement Group
Connection Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress message length average (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is updated for each egress message during the Tx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

TxAllLenPeak

Measurement ID
18049

Measurement Group
Connection Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress message length peak (routable and peer-to-peer).

Collection Interval
5 min

Peg Condition
This measurement is updated for each egress message during the Tx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

TxConnTotalDataChunks

Measurement ID
10507

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of total data chunks sent on the SCTP connection.

Collection Interval
5 min

Peg Condition
When data chunks are transmitted on the SCTP connection.

Measurement Scope
Server Group

Recovery

1. No action required.

TxP0

Measurement ID
18038

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress messages with priority 0.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each ingress message with priority 0 during the Message Priority phase.

Measurement Scope
Site

Recovery

1. No action required.

TxP1

Measurement ID
18046

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress messages with priority 1.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message with priority 1 during the Tx phase.

Measurement Scope
Site

Recovery

1. No action required.

TxP2

Measurement ID
18047

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress messages with priority 2.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message with priority 2 during the Tx phase.

Measurement Scope
Site

Recovery

1. No action required.

TxP3

Measurement ID
10154

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress messages with priority 3.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message with priority 3 during the Tx phase.

Measurement Scope
Site

Recovery

1. No action required.

TxP4

Measurement ID
18068

Measurement Group
Connection Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress messages with priority 4.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each egress message with priority 4 during the Tx phase.

Measurement Scope
Site

Recovery

1. No action required.

Connection Service measurements

EvException

Measurement ID
18007

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection exception events.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each EvException event, regardless of event reason or throttling.

Measurement Scope
Site

Recovery

1. No action required.

EvFsmAdState

Measurement ID
18004

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection FSM administrative state change events.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each EvFsmAdState event, regardless of event reason or throttling.

Measurement Scope
Site

Recovery

1. No action required.

EvFsmException

Measurement ID
18006

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection FSM exception events.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each EvFsmException event, regardless of event reason or throttling.

Measurement Scope
Site

Recovery

1. No action required.

EvFsmOpState

Measurement ID
18005

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection FSM operational state change events.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each EvFsmOpState event, regardless of event reason or throttling.

Measurement Scope
Site

Recovery

1. No action required.

TmFsmOpStateAvailable

Measurement ID
10150

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for operational state available.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is operationally available.

Measurement Scope
Site

Recovery

1. No action required.

TmFsmOpStateDegraded

Measurement ID
10183

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for operational state degraded.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is operationally degraded.

Measurement Scope
Site

Recovery

1. No action required.

TmFsmOpStateUnavailable

Measurement ID
10182

Measurement Group
Connection Service

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection timer for operational state unavailable.

Collection Interval
5 min

Peg Condition
This measurement is incremented for each millisecond the connection is operationally unavailable.

Measurement Scope
Site

Recovery

1. No action required.

Connection Transport measurements

The Connection Transport measurement report contains measurements that provide performance information that is specific to the DCL at the connection level.

RxBufAvg

Measurement ID
10106

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress buffer utilization average.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

RxBufPeak

Measurement ID
10107

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection ingress buffer utilization peak.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

RxOctets

Measurement ID
10105

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection ingress octets.

Collection Interval
5 min

Peg Condition
This measurement is updated for each ingress message during the Rx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

RxSctpChunk

Measurement ID
10516

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
SCTP total chunks on ingress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

RxSctpDupTsn

Measurement ID
10504

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
SCTP duplicate TSNs on ingress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

RxSctpGapAck

Measurement ID
10505

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
SCTP gap acknowledgement on ingress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

RxTcpDupPkt

Measurement ID
10508

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
TCP duplicate packets on ingress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

TxBufAvg

Measurement ID
10102

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress buffer utilization average.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

> **Note:** This measurement is not supported (always zero) for SCTP connections.

Measurement Scope
Site

Recovery

1. No action required.

TxBufPeak

Measurement ID
10103

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Connection egress buffer utilization peak.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

> **Note:** This measurement is not supported (always zero) for SCTP connections.

Measurement Scope
Site

Recovery

1. No action required.

TxOctets

Measurement ID
10101

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Connection egress octets.

Collection Interval
5 min

Peg Condition
This measurement is updated for each egress message during the Tx phase (routable and peer-to-peer).

Measurement Scope
Site

Recovery

1. No action required.

TxSctpChunk

Measurement ID
10507

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
SCTP total chunks on egress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

TxSctpRtxChunk

Measurement ID
10506

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
SCTP retransmitted chunks on egress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

TxTcpRtxSeg

Measurement ID
10509

Measurement Group
Connection Transport

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
TCP retransmitted segments on egress.

Collection Interval
5 min

Peg Condition
Output from Linux networking stack.

Measurement Scope
Site

Recovery

1. No action required.

Diameter Egress Transaction measurements

The Diameter Egress Transaction measurement report contains measurements providing information about Diameter peer-to-peer transactions forwarded to upstream peers.

RxAnswerExpectedAll

Measurement ID
10040

Measurement Group
Diameter Egress Transaction, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.

Collection Interval
5 min

Peg Condition
When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction is found.

The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxAnswerMsgQueueFullDiscard

Measurement ID
10232

Measurement Group
Diameter Egress Transaction, Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.

Collection Interval
5 min

Peg Condition
For each Answer message discarded because the Answer Message Queue was full.

The connection measurement is associated with the connection from which the message was received.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

RxRedirectHostNotRouted

Measurement ID
14071

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Redirect Host Notifications received for which a Redirected Request was not submitted for rerouting.

Collection Interval
5 min

Peg Condition
When **DRL**, for any reason, does not submit the Redirected Request message for routing.

The connection measurement is associated with the connection from which the Redirect Notification was received.

Measurement Scope
Site

Recovery

1. No action required.

RxRedirectHostRouted

Measurement ID
14070

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Redirect Host Notifications received for which the Redirect-Host AVP has been updated and submitted for rerouting.

Collection Interval
5 min

Peg Condition
When **DRL** successfully queues a Redirected Request message for routing.

The connection measurement is associated with the Connection from which the Redirect Notification was received.

Measurement Scope
Site

Recovery

1. No action required.

RxRedirectRealmNotRouted

Measurement ID
14073

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Redirect Realm Notifications received for which a Redirected Request was not submitted for rerouting.

Collection Interval
5 min

Peg Condition
When **DRL**, for any reason, does not submit the Redirected Request message for routing.

The connection measurement is associated with the connection from which the Redirect Notification was received.

Measurement Scope
Site

Recovery

1. No action required.

RxRedirectRealmRouted

Measurement ID
14072

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Redirect Realm Notifications received for which the Redirect-Host AVP has been updated and submitted for rerouting.

Collection Interval
5 min

Peg Condition
When **DRL** successfully queues a Redirected Request message for routing.

The connection measurement is associated with the connection from which the Redirect Notification was received.

Measurement Scope
Site

Recovery

1. No action required.

TxAnswerTimeout

Measurement ID
10044

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of times that an Answer response was not received from a peer before the maximum allowed time defined by the “Pending Answer Timer” value.

Answer timeouts can be caused by a variety of reasons:

- The peer associated with this connection may be experiencing congestion, causing delays in sending the Answer response.
- IP Network congestion.
- If the peer associated with this connection is a Diameter **Relay Agent**, then an upstream node from the peer may be experiencing congestion, causing delays in sending the Answer response.

Collection Interval
5 min

Peg Condition
When timer PENDING-ANSWER-TIMER expires.

The connection measurement is associated with the connection from which the corresponding Request message was sent.

Measurement Scope
Server Group

Recovery

1. If the user-configurable answer response timer is set too low it can cause the timer to expire before a Answer response is received. The user-configurable value is set using the page **Diameter** > **Configuration** > **System Options**.
2. It is recommended to contact My Oracle Support for assistance if needed.

TxAnswerTimeoutAllMp

Measurement ID
14075

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of times that an Answer response was not received from a peer before the maximum allowed time defined by the "Pending Answer Timer" value.

Collection Interval
5 min

Peg Condition
When timer PENDING-ANSWER-TIMER expires.

The connection measurement is associated with the connection from which the corresponding Request message was sent.

Note: This measurement is the DA-MP equivalent to the "per connection" measurement TxAnswerTimeout.

Measurement Scope
Site

Recovery

1. If the user-configurable answer response timer is set too low it can cause the timer to expire before a Answer response is received. The user-configurable value is set using the page **Diameter** > **Configuration** > **System Options**.
2. It is recommended to contact My Oracle Support for assistance if needed.

TxAnswerTimeoutMp

Measurement ID
14075

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of times that an Answer response was not received from a peer before the maximum allowed time defined by the "Pending Answer Timer" value.

Collection Interval
5 min

Peg Condition
When timer PENDING-ANSWER-TIMER expires. The connection measurement is associated with the connection from which the corresponding Request message was sent.

Note: This is the DA-MP equivalent to the "per connection" measurement, TxAnswerTimeout.

Measurement Scope
Site

Recovery

1. If the user-configurable answer response timer is set too low it can cause the timer to expire before an Answer response is received. The user-configurable value is set using the page **Diameter** > **Configuration** > **System Options**.
2. It is recommended to contact My Oracle Support for assistance if needed.

TxConnectionFailed

Measurement ID
10046

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of times that a pending peer-to-peer transaction was abandoned due to a transport connection failure.

Collection Interval
5 min

Peg Condition
When a pending transaction is rerouted due to a transport connection failure.

This connection measurement is associated with the connection to which the corresponding Request message was sent.

Measurement Scope
Server Group

Recovery

1. Connection status can be monitored using the **Diameter** > **Maintenance** > **Connections** page.
2. It is recommended to contact My Oracle Support for assistance if needed.

TxConnAnswerMsgs

Measurement ID
10154

Measurement Group
Diameter Egress Transaction, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of routable Answer messages successfully sent on the connection.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter Answer message is sent to the peer.

Measurement Scope
Server Group

Recovery

1. No action required.

TxConnRequestMsgs

Measurement ID
10153

Measurement Group
Diameter Egress Transaction, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of routable Request messages successfully sent on the connection.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter request message is sent to the peer.

Measurement Scope
Server Group

Recovery

1. No action required.

TxRequestSuccessAllConn

Measurement ID
10043

Measurement Group
Diameter Egress Transaction

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages successfully routed to a peer.

Collection Interval
5 min

Peg Condition
When the DSR successfully queues a Request message to the DCL.

The connection measurement is associated with the connection to which the Request message was sent.

Measurement Scope
Server Group

Recovery

1. No action required.

Diameter Exception measurements

The Diameter Exception measurement report contains measurements that provide information about exceptions and unexpected messages and events that are specific to the Diameter protocol.

EvAppIdListInconsistency

Measurement ID
10009

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of times that the supported Application IDs received from the peer were inconsistent with another transport connection.

Collection Interval
5 min

Peg Condition
If the Application ID list received from the DSR for a peer's transport connection is not identical to the Application ID list for at least one of the transport connections for a peer that has an Operation Status state of Available.

Measurement Scope
Server Group

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 DSR 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, it is recommended to contact My Oracle Support.

EvTransLifetimeExceededMp

Measurement ID
10098

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of transaction failures because “Transaction Lifetime” exceeded.

Collection Interval
5 min

Peg Condition
When the **DRL** was prevented from rerouting a Request message because the “Transaction Lifetime” was exceeded.

Measurement Scope
Site

Recovery

1. No action required.

EvTransRejectedByExternalNode

Measurement ID
14068

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of transactions rejected by an external node with a non-2xxx Result-Code value.

Collection Interval
5 min

Peg Condition
When DSR successfully relays an answer response received from an upstream external node to a downstream external node and the answer contains a failure response (i.e., a Result-Code AVP value not in the range of 2000-2099)

Note: This measurement is not pegged for answer generated by application.

Measurement Scope
Server Group

Recovery

1. No action required.

RxAnswerMsgQueueFullDiscard

Measurement ID
10232

Measurement Group
Diameter Egress Transaction, Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.

Collection Interval
5 min

Peg Condition
For each Answer message discarded because the Answer Message Queue was full.

The connection measurement is associated with the connection from which the message was received.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

RxAnswerUnexpected

Measurement ID
10008

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.

Collection Interval
5 min

Peg Condition
When the DRL receives an Answer message event from DCL/RCL with a valid transport connection ID for which a pending transaction is found.

The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxAnswerUnexpectedAllMp

Measurement ID
14064

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Answer messages received from an upstream peer that could not be associated with a pending transaction.

Collection Interval
5 min

Peg Condition
When DRL receives an answer message event from DCL/RCL with a valid Diameter Connection ID for which a pending transaction cannot be found

The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxDOCRejectMp

Measurement ID
10251

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress messages that were rejected with error answer due to local DA-MP danger of CPU congestion.

Collection Interval
5 min

Peg Condition
Pegged for each message discarded with a DIAMETER (Error) Answer due to DA-MP danger of CPU congestion.

Measurement Scope
Server Group

Recovery

1. The **DA-MP** is approaching or exceeding its maximum configured MPS limitation. If this value is not set to the MP's engineered traffic handling capacity, then the maximum MPS capacity allowed may need to be changed.
2. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. **DA-MP** server status can be monitored from the **Status & Manage** > **Server** page.
3. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each **DA-MP** can be monitored from the **Status & Manage** > **KPIs** page. Each **DA-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. The ingress traffic rate of each **DA-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.
5. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, it is recommended to contact My Oracle Support.

RxMsgsOCGreenPri0DiscardMp

Measurement ID
10276

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Green ingress Priority 0 messages discarded by the **DA-MP** Overload Control component.

Collection Interval
5 min

Peg Condition
Each time a Priority 0 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component

Measurement Scope
Site

Recovery

1. If one or more **MPs**s 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, it is recommended to contact My Oracle Support.

RxMsgsOCYellowPri0DiscardMp

Measurement ID
10277

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Yellow ingress Priority 0 messages discarded by the **DA-MP** Overload Control component.

Collection Interval
5 min

Peg Condition
Each time a Priority 0 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component

Measurement Scope
Site

Recovery

1. If one or more **MP**s 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, it is recommended to contact My Oracle Support.

RxMsgsOCGreenPri1DiscardMp

Measurement ID
10278

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Green ingress Priority 1 messages discarded by the **DA-MP** Overload Control component.

Collection Interval
5 min

Peg Condition
Each time a Priority 1 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component

Measurement Scope
Site

Recovery

1. If one or more **MP**s 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, it is recommended to contact My Oracle Support.

RxMsgsOCYellowPri1DiscardMp

Measurement ID
10279

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Yellow ingress Priority 1 messages discarded by the **DA-MP** Overload Control component.

Collection Interval
5 min

Peg Condition
Each time a Priority 1 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component

Measurement Scope
Site

Recovery

1. If one or more **MP**s 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, it is recommended to contact My Oracle Support.

RxMsgsOCGreenPri2DiscardMp

Measurement ID
10280

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Green ingress Priority 2 messages discarded by the **DA-MP** Overload Control component.

Collection Interval
5 min

Peg Condition
Each time a Priority 2 Diameter Request message marked "Green" arrives at the DA-MP Overload Control component

Measurement Scope
Site

Recovery

1. If one or more **MP**s 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, it is recommended to contact My Oracle Support.

RxMsgsOCYellowPri2DiscardMp

Measurement ID
10281

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Yellow ingress Priority 2 messages discarded by the **DA-MP** Overload Control component.

Collection Interval
5 min

Peg Condition
Each time a Priority 2 Diameter Request message marked "Yellow" arrives at the DA-MP Overload Control component

Measurement Scope
Site

Recovery

1. If one or more **MP**s 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, it is recommended to contact My Oracle Support.

TmConnDegraded

Measurement ID
10183

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Total time (in seconds) during the reporting period that the connection state was in the Degraded state.

Collection Interval
5 min

Peg Condition
Pegging started when a peer enters the Degraded state. Pegging stopped when the peer enters the Available or Unavailable state.

A peer may be degraded for short periods of time (< 30 seconds) due to being in a proving period or during a graceful disconnect; degraded conditions lasting longer periods of time are most likely due to local congestion.

Measurement Scope
Server Group

Recovery

1. If this measurement indicates an excessive amount of time spent in the degraded state, examine the Alarm History to determine the cause of the degraded condition.
2. It is recommended to contact My Oracle Support for assistance if needed.

TmConnEnabledNotAvail

Measurement ID
10182

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Total time (in seconds) during the reporting period that the connection state was administratively enabled and the connection state was not Available.

Collection Interval
5 min

Peg Condition
Pegging is started when a peer is enabled or when a peer disconnects. Pegging is stopped when the peer connects and completes capabilities exchange, or when the connection is disabled.

Measurement Scope
Server Group

Recovery

1. Examine the Alarm History to determine if the connection is being rejected by either end, and for notification of local congestion.
2. Make sure the peer is running.
3. If the connection is configured as a Responder connection, make sure that the peer is attempting to initiate a connection.
4. If the connection is an Initiator connection, make sure that the peer is listening on the configured port.
5. It is recommended to contact My Oracle Support for assistance if needed.

TxDtlsOversizedDiscard

Measurement ID
10515

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of oversized egress messages discarded on the **DTLS** connection.

Collection Interval
5 min

Peg Condition
When the message size to be sent on the DTLS connection is greater than 16K (16384) bytes.

Measurement Scope
Server Group

Recovery

1. No action required.

TxReqMsgPerConnPtrMax

Measurement ID
10007

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of times message routing bypassed the connection because the maximum allowed pending transactions was exceeded.

Collection Interval
5 min

Peg Condition
Each time the DSR bypasses a transport connection during route selection because the maximum number of pending transactions allowed for the connection was exceeded.

The connection measurement is pegged against the egress connection with the maximum number of pending transactions condition which prevented message routing.

Measurement Scope
Server Group

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 DSR 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, it is recommended to contact My Oracle Support.

TxRequestEgressLoop

Measurement ID
10005

Measurement Group
Diameter Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of times that a selected route associated with an egress peer was not selected because a forwarding loop would occur (i.e., the upstream peer has already processed the Request message as determined by the Route-Record AVPs).

Collection Interval
5 min

Peg Condition
Each time the DSR bypasses a peer during route selection because the peer's FQDN matches one of the FQDNs in the message's Route-Record AVPs.

The connection measurement is associated with the first connection assigned to the peer.

Note: This failure is associated with the peer, not any particular connection. The measurement should always be pegged against the same peer connection, i.e., the first one assigned to the peer.

Measurement Scope
Server Group

Recovery

1. It is recommended to contact My Oracle Support for assistance if needed.

Diameter Ingress Transaction Exception measurements

The Diameter Ingress Transaction Exception report group contains measurements providing information about exceptions associated with the routing of Diameter transactions received from downstream peers.

RxArtRuleRejection

Measurement ID
14067

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Diameter Connection ID)

Description
The number of Request messages from a downstream peer rejected by a local node because an application routing rule Action is set to 'Send Answer" or "Abandon with No Answer".

Collection Interval
5 min

Peg Condition
Each time a Request message from a downstream peer is rejected by a Local node because an application routing rule Action is set to "Send Answer".

> **Note:** The "connection measurement" is associated with the Diameter Connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action necessary

RxDecodeFailure

Measurement ID
10031

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of Request messages rejected from a downstream peer because the message could not be decoded.

Collection Interval
5 min

Peg Condition
Request message from a downstream peer is rejected by a Local Node because it could not be decoded.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. These protocol violations are caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer that forwarded the message to this node (identified by the peer name) and cannot be fixed using the application.
2. It is recommended to contact My Oracle Support for assistance if needed.

RxDOCDiscardMp

Measurement ID
10252

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress messages that were discarded due to local DA-MP danger of CPU congestion.

Collection Interval
5 min

Peg Condition
Pegged for each message discarded due to DA-MP danger of CPU congestion.

Measurement Scope
Server Group

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. **DA-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 **DA-MP** can be monitored from the **Status & Manage** > **KPIs** page. 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. The ingress traffic rate of each **DA-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, it is recommended to contact My Oracle Support.

RxMessageLooping

Measurement ID
10032

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages from a downstream peer rejected by a Local Node because message looping was detected (FQDN of the Local Node associated with the ingress transport connection matched a FQDN in the messages' Route-Record AVPs).

Collection Interval
5 min

Peg Condition
Request message from a downstream peer is rejected by a Local Node with Result-Code 3005 (DIAMETER_LOOP_DETECTED).

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer timeouts. The status of connections should be examined from the **Diameter** > **Maintenance** > **Connections** page.
2. If no additional congestion alarms are asserted, the routing Answer task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If the problem persists, it is recommended to contact My Oracle Support.

RxNoRoutesFound

Measurement ID
10035

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of Request messages from a downstream peer rejected by a Local Node because no routes were available for routing the message.

Collection Interval
5 min

Peg Condition
Request message from a downstream peer is rejected by a Local Node because no routes were available for routing the message. A No Routes Available condition occurs when:

- A Route List was selected via a Peer Routing Rule or implicit routing but its Operational Status was Unavailable
- Implicit routing was invoked and the peer's Operational Status was not Available and an alternate implicit route was not provisioned for the peer

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. If the message matched a Peer Routing Rule but none of the peers in the Route List were eligible for routing the message because either their operation state was Unavailable, the Application ID in the Request message did not match an application ID supported by the peer, or the peer had previously processed the message as defined by the Route-Record AVPs in the message:
   a. Verify that IP network connectivity exists between the MP server and the peers.
   b. Check the event history logs for additional DIAM events or alarms from this **MP** server.
   c. Verify that the peers in the Route List are not under maintenance. It is recommended to contact My Oracle Support for assistance if needed.
2. If the message was addressed to a peer directly connected to the Local Node via the Destination-Host AVP but the peer's operational status was Unavailable or the alternate path to the peer, designated by the peer's alternate implicit route was either not provisioned or was Unavailable:
   a. Verify that IP network connectivity exists between the MP server and the adjacent servers.
   b. Check the event history logs for additional DIAM events or alarms from this **MP** server.
   c. Verify that the peer is not under maintenance.
3. If the message was addressed to a peer directly connected to the Local Node via the Destination-Host AVP but the application ID in the Request message did not match an Application ID supported by the peer:
   a. 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.
   b. 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.

c. 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.

4. It is recommended to contact My Oracle Support for assistance if needed.

RxNoRulesFailure

Measurement ID
10034

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages from a downstream peer rejected by a Local Node because no Peer Routing Rule was found.

Collection Interval
5 min

Peg Condition
Request message from a downstream peer is rejected by a Local Node because no Peer Routing Rules were found in the peer routing table and the message was not addressed to a peer (either Destination-Host AVP was absent or Destination-Host AVP was present but was not a peer's FQDN) or a configured Realm/Application-Id (via the Realm Route Table).

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

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 Routing 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, it is recommended to contact My Oracle Support.

RxPrtRuleRejection

Measurement ID
10037

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages from a downstream peer rejected by a Local Node because a Peer Routing Rule action is set to "Send Answer" or "Abandon with No Answer".

Collection Interval
5 min

Peg Condition
Request message from a downstream peer rejected by a Local Node because a Peer Routing Rule action is set to "Send Answer" or "Abandon with No Answer".

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Site

Recovery

1. No action required.

RxRejectedAll

Measurement ID
10030

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages rejected from a downstream peer by a Local Node (all reasons).

Collection Interval
5 min

Peg Condition
When measurement RxRejectedConnCongestion, RxDecodeFailure, RxMessageLooping, RxAllDrop, RxNoRulesFailure, RxNoRoutesFound, RxTransactionTimeout, RxPrtRuleRejection, or RxRejectedOther is pegged.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRejectedOther

Measurement ID
10038

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages from a downstream peer rejected by a Local Node for any reason other than those identified by measurements RxDecodeFailure, RxMessageLooping, RxAllDrop, RxNoRulesFailure, RxNoRoutesFound, RxTransactionTimeout, RxArtRuleRejection, or RxPrtRuleRejection.

Collection Interval
5 min

Peg Condition
Request message from a downstream peer rejected by a Local Node for any reason other than those identified by measurements RxDecodeFailure, RxMessageLooping, RxAllDrop, RxNoRulesFailure, RxNoRoutesFound, RxTransactionTimeout, RxArtRuleRejection, or RxPrtRuleRejection.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRequestMsgQueueFullDiscard

Measurement ID
10231

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress Diameter Request messages that were discarded because the Request Message Queue was full.

Collection Interval
5 min

Peg Condition
For each Request message discarded because the Request Message Queue was full.

The connection measurement is associated with the connection from which the message was received.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

RxTransactionTimeout

Measurement ID
10036

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages from a downstream peer rejected by a Local Node because maximum message reroutes are exceeded.

Collection Interval
5 min

Peg Condition
Request message from a downstream peer is rejected by a Local Node because maximum number of message reroutes was exceeded.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. If the maximum number of message reroutes is set too low (e.g., zero) then any failure trigger message reroute will fail. The user-configurable value is set using the **Diameter** > **Configuration** > **System Options** page.
2. If the user-configurable answer response timer is set too low the timer expires before an Answer response is received. The user-configurable value is set using the **Diameter** > **Configuration** > **System Options** page.
3. It is recommended to contact My Oracle Support for assistance if needed.

TxLongTimeoutPtrListEmpty

Measurement ID
10296

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress Diameter Request messages that were discarded because no Long Timeout PTR Buffers were available.

Collection Interval
5 min

Peg Condition
When any DRL thread within the Diameter Process needs to allocate a Long Timeout PTR Buffer from the Long Timeout PTR Buffer Pool and the number of allocated Long

Timeout PTRs from a Long Timeout PTR Buffer Pool is less than the maximum configured capacity of Long Timeout PTR Buffers then:

- A Long Timeout PTR Buffer shall be allocated from the Long Timeout PTR Buffer Pool
- The count for the number of allocated Long Timeout PTRs from a Long Timeout PTR Buffer Pool shall be incremented by one.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP when the Ingress Message Rate and/or Diameter Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. If the problem persists, it is recommended to contact My Oracle Support.

TxPtrListEmpty

Measurement ID
10228

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress Diameter Request messages that were discarded because no PTR Buffers were available.

Collection Interval
5 min

Peg Condition
When any DRL thread within the Diameter Process needs to allocate a PTR Buffer from the PTR Buffer Pool and the number of allocated PTRs from a PTR Buffer Pool is less than the maximum configured capacity of PTR Buffers then:

- A PTR Buffer shall be allocated from the PTR Buffer Pool

- The count for the number of allocated PTRs from a PTR Buffer Pool shall be incremented by one.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** when the Ingress Message Rate and/or Diameter Process CPU Utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. It is recommended to contact My Oracle Support for assistance if needed.

TxRerouteQueueFullReject

Measurement ID
10241

Measurement Group
Diameter Ingress Transaction Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of egress Diameter Request messages that were rejected because the Reroute Queue was full.

Collection Interval
5 min

Peg Condition
For each Request message rejected because the Reroute Queue was full.

The connection measurement is associated with the connection the Request message was received from.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of

an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

Diameter Ingress Transaction Performance measurements

The Diameter Ingress Transaction Performance measurement report contains measurements providing information about the outcome of Diameter transactions received from downstream peers.

RxConnRequestMsgs

Measurement ID
10151

Measurement Group
Diameter Ingress Transaction Performance, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of routable Request messages received on the connection.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter request message is received from the peer.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswer1xxx

Measurement ID
10020

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 1xxx.

Collection Interval
5 min

Peg Condition
Answer message received from a peer that was successfully sent to the DCL/RCL with a Result-Code value in the range of 1000 - 1999.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswer2xxx

Measurement ID
10021

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 2xxx.

Collection Interval
5 min

Peg Condition
Answer message received from a peer that was successfully sent to the DCL/RCL with a Result-Code value in the range of 2000 - 2999.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswer3xxx

Measurement ID
10022

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 3xxx (Protocol Error).

Collection Interval
5 min

Peg Condition
Answer message received from a peer that was successfully sent to the DCL//RCL with a Result-Code value in the range of 3000 - 3999.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswer4xxx

Measurement ID
10023

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 4xxx (Transient Failure).

Collection Interval
5 min

Peg Condition
Answer message received from a peer that was successfully sent to the DCL/RCL with a Result-Code value in the range of 4000 - 4999.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswer5xxx

Measurement ID
10024

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value 5xxx (Permanent Failure).

Collection Interval
5 min

Peg Condition
Answer message received from a peer that was successfully sent to the DCL/RCL with a Result-Code value in the range of 5000 - 5999.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswerFailure

Measurement ID
10027

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of (expected) Answer responses from a peer and Answer responses created by a Local Node which were not successfully routed to a downstream peer (for any reason).

> **Note:** An expected Answer response from a peer is an Answer response for which a pending transaction existed.

Collection Interval
5 min

Peg Condition
Any time the DCL/RCL fails to queue an Answer response.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswerLocalNode

Measurement ID
10026

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from a Local Node that were successfully routed to a downstream peer (all Result-Code values).

Collection Interval
5 min

Peg Condition
Any time the DCL/RCL successfully creates and queues an Answer response to DCL in response to a Request message received from a downstream peer.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

TxAnswerOther

Measurement ID
10025

Measurement Group
Diameter Ingress Transaction Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Answer responses from peers that were successfully routed to a downstream peer with a Result-Code value not in the range of 1000-5999.

Collection Interval
5 min

Peg Condition
Answer message received from a peer which was successfully sent to the DCL/RCL with either a Result-Code value not in the range of 1000 - 5999 or without a Result-Code AVP.

The connection measurement is associated with the connection to which the message was routed.

Measurement Scope
Server Group

Recovery

1. No action required.

Diameter Performance measurements

The Diameter Performance measurement report contains measurements that provide performance information that is specific to the Diameter protocol.

EvPerConnPtrQueueAvg

Measurement ID
10240

Measurement Group
Diameter Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
The average length of the PTR queue for a connection during the collection interval.

Collection Interval
5 min

Peg Condition
Each time a PTR is dequeued or enqueued on the connection's PTR queue, the average queue length is calculated using the **COMCOL** average measurement type method.

Measurement Scope
Server Group

Recovery

1. No action required.

EvPerConnPtrQueuePeak

Measurement ID
10239

Measurement Group
Diameter Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Connection ID)

Description
The maximum length of the PTR queue for a connection during the collection interval.

Collection Interval
5 min

Peg Condition
Each time a PTR is dequeued or enqueued on the connection's PTR queue, the maximum queue length is calculated using the COMCOL maximum measurement type method.

Measurement Scope
Server Group

Recovery

1. No action required.

EvRemoteBusy

Measurement ID

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension

Description
Number of times that a connection's Remote Busy State changed from "Not Busy" to "Busy".

Collection Interval
5 min

Peg Condition
Each time that DRL changes the connection's "Remote Busy State" to "Busy".

Measurement Scope
Server Group

Recovery

1. Use **Main Menu** > **Diameter** > **Configuration** > **Connections** to examine and modify the "Remote Busy Abatement Timeout" attribute setting for the connection.

   If the total duration that the connection is congested is small (as defined by TmRemoteBusy), then the user-configurable "Remote Busy Abatement Timeout" attribute for the connection may be set too small.

2. The ingress message rate to the connection is excessive.

3. It is recommended to contact My Oracle Support for assistance if needed.

EvTransSuccessByExternalNode

Measurement ID
14069

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of transactions where an external node sends success (2xxx) Answer to Diameter Node.

Collection Interval
5 min

Peg Condition
When DSR successfully relays an answer response received from upstream external node to a downstream external node and the answer contains a success response (i.e. a Result-Code AVP value in the range of 2000-2999)

Measurement Scope
Server Group

Recovery

1. No action required.

MpEvRadiusRoutedMsgs

Measurement ID
14074

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress RADIUS messages processed by DRL, including Rerouting and Message Copy.

Collection Interval
5 min

Peg Condition
This measurement should be incremented as per the following conditions.

- Ingress RADIUS Request processing resulting in a Request being routed upstream (with or without local DSR application processing of the Request)
- Ingress RADIUS Response processing resulting in forwarding of Answer/ Response downstream (with or without local DSR application processing of the Response)
- Ingress Request processing resulting in Answer message sent by DSR to originator (with or without local DSR application processing of the Request)

- Ingress RADIUS Request discarded due to validation error or overload
- Ingress RADIUS Response discarded due to validation error
- Initial copy and transmit of a RADIUS Request to a DAS
- Ingress RADIUS Response triggering reroute of the pending Request message (including Answers from DAS for copied RADIUS Requests)
- RADIUS Request reroute due to connection failure or Answer/Response timeout (including reroute of copied Requests to DAS for same reasons)
- Ingress Answer from a DAS terminated by DSR due to RADIUS Request copy completion or termination

Note: This is the functional equivalent to RoutingMsgs but for ingress RADIUS (only) messages. Measurement RoutingMsgs measures all ingress equivalent messages (Diameter and RADIUS).

Measurement Scope
Network

Recovery

1. No action required.

RoutingMsgs

Measurement ID
10243

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Diameter and RADIUS messages processed by DRL, including Rerouting and Message Copy.

Collection Interval
5 min

Peg Condition
This measurement should be incremented as per the following conditions.

- Ingress RADIUS Request processing resulting in a Request being routed upstream (with or without local DSR application processing of the Request)

- Ingress RADIUS Response processing resulting in forwarding of Answer/ Response downstream (with or without local DSR application processing of the Response)
- Ingress Request processing resulting in Answer message sent by DSR to originator (with or without local DSR application processing of the Request)
- Ingress RADIUS Request discarded due to validation error or overload
- Ingress RADIUS Response discarded due to validation error
- Initial copy and transmit of a RADIUS Request to a DAS
- Ingress RADIUS Response triggering reroute of the pending Request message (including Answers from DAS for copied RADIUS Requests)
- RADIUS Request reroute due to connection failure or Answer/Response timeout (including reroute of copied Requests to DAS for same reasons)
- Ingress Answer from a DAS terminated by DSR due to RADIUS Request copy completion or termination

Measurement Scope
Network

Recovery

1. No action required.

RxAnswerExpectedAll

Measurement ID
10040

Measurement Group
Diameter Egress Transaction, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.

Collection Interval
5 min

Peg Condition
When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction is found.

The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxAnswerExpectedAllMp

Measurement ID
10091

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of valid Answer messages received from an upstream peer that were associated with a pending transaction.

Collection Interval
5 min

Peg Condition
When the **DSR** receives an Answer message event with a valid transport connection ID for which a pending transaction is found.

The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxAnswerExpectedRoutedMp

Measurement ID
10092

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of valid Answer messages received from an upstream peer that were successfully routed to a downstream peer.

Collection Interval
5 min

Peg Condition

Measurement Scope
Server Group

Recovery

1. No action required.

RxConnRequestMsgs

Measurement ID
10151

Measurement Group
Diameter Ingress Transaction Performance, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of routable Request messages received on the connection.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter request message is received from the peer.

Measurement Scope
Server Group

Recovery

1. No action required.

RxDiam2DiamTransactionsCount

Measurement ID
14065

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The total number of Diameter to Diameter transactions

Collection Interval
5 min

Peg Condition
When an answer message is received from an upstream peer or an answer message is generated by DRL to downstream peer for which pending transaction record has been allocated previously

Measurement Scope
Server Group

Recovery

1. No action required.

RxRequestMsgsMp

Measurement ID
10131

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Request messages received.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter request message received is from the peer. This measurement is pegged for all requests accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRequestNoErrors

Measurement ID
10003

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of transactions successfully processed on one routing attempt.

Collection Interval
5 min

Peg Condition
When an Answer response from a peer is successfully queued to the DCL/RCL for a transaction and the total number of times that the corresponding Request message has been forwarded to a peer equals "1".

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required

RxRequestNoErrorsMp

Measurement ID
10094

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of transactions successfully processed on one routing attempt.

Collection Interval
5 min

Peg Condition
When an Answer response from a peer is successfully queued to the DSR for a transaction and the total number of times that the corresponding Request message has been forwarded to a peer equals "1".

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

TmConnAvail

Measurement ID
10150

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Total time in seconds that the connection state was available during the measurement period.

Collection Interval
5 min

Peg Condition
Pegging started when the connection state is Available. Pegging stopped when the connection state is Unavailable or Degraded.

Measurement Scope
Server Group

Recovery

1. If this measurement varies significantly from the total time in the collection period, examine the Alarm History to determine the reason(s) that the connection was Unavailable or Degraded.
2. It is recommended to contact My Oracle Support for assistance if needed.

TmHoldTimeDownstreamMp

Measurement ID
14066

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The time (in milliseconds) from when a pending transaction record is allocated by DRL and until DRL stops processing the transaction and deallocates the PTR.

Collection Interval
5 min

Peg Condition

- The time interval for each transaction starts when DRL allocates and stores PTR for an ingress Request message from a downstream peer
- The time interval for each transaction when DRL stops processing and the transaction deallocates the PTR and sends an answer response to DCL

This includes Answer messages received from an upstream peers and those generated by DRL.

Measurement Scope
Server Group

Recovery

1. No action required.

TmRemoteBusy

Measurement ID
10042

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed

Description
Total time (in milliseconds) that a connection's Remote Busy State was Busy.

Collection Interval
5 min

Peg Condition
Each time that DRL changes the connection's Remote Busy State to Busy. Each time interval stops when DRL changes the connection's Remote Busy State to Not Busy

Measurement Scope
Server Group

Recovery

1. The ingress message rate to the connection is excessive.

   Under normal circumstances, TmRemoteBusy should be very small. If it is large, then the ingress message traffic to the connection may be exceeding the ability of the peer to process the traffic from this connection. The following measurements may be useful in evaluating the ingress traffic for this connection:

   - TxAll - measures the total routable and non-routable measurements which were sent on the connection.
   - TxRequestSuccessAllConn - measures the total number of Request messages forwarded to the connection.

   a. An excessive number of messages may have been rerouted to this connection. Examine TxRerouteAttempts, TxRerouteConnFailure, TxRerouteAnswerTimeout, TxRerouteSuccessSent, and RxRerouteAnswerRsp.

   b. Route Group configurable options can be viewed and modified using **Main Menu** > **Diameter** > **Configuration** > **Route Groups**.

      The connection may be a member of one or more Route Groups whose peer or connection weight may be mis-configured or need modification.

   c. Use **Main Menu** > **Diameter** > **Configuration** > **Route Groups** to examine Connection status.

      The connection may be a member of one or more Route Groups containing failed connections. When this occurs, the traffic will be routed to the remaining connections in those route groups.

   d. The peer node or this particular connection to the peer node may be under-engineered for the ingress traffic load.

   e. The total offered load to this connection may have peaked during a short time duration due to larger than normal network usage patterns. This measurement should be view over multiple measurement intervals to look for trends.

2. Use **Main Menu** > **Diameter** > **Configuration** > **Connections** to examine and modify the Remote Busy Abatement Timeout attribute setting for the connection.

   If the total duration that the connection is congested is small (as defined by TmRemoteBusy), then the user-configurable Remote Busy Abatement Timeout attribute for the connection may be set too small.

3. It is recommended to contact My Oracle Support for assistance if needed.

TmResponseTimeDownstream

Measurement ID
10001

Measurement Group
Diameter Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
Average time (in milliseconds) from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer.

Collection Interval
5 min

Peg Condition
Time interval for each transaction starts when the DRL successfully decodes an ingress Request message from a downstream peer. Time interval for each transaction stops when the DRL attempts to send an Answer response to the DCL/RCL. This includes Answer messages received from upstream peers and those generated by the DRL.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. If the average is significantly larger than what is considered normal, then additional measurements, such as measurement TmResponseTimeUpstream, should be consulted to assist in determining the source of the delay.
2. It is recommended to contact My Oracle Support for assistance if needed.

TmResponseTimeDownstreamMp

Measurement ID
10093

Measurement Group
Diameter Performance

Measurement Type
Average

Measurement Dimension
Single

Description
Average time (in milliseconds) from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer.

Collection Interval
5 min

Peg Condition
Time interval for each transaction starts when the DSR successfully decodes an ingress Request message from a downstream peer. Time interval for each transaction stops when the DSR attempts to send an Answer response. This includes Answer messages received from upstream peers and those generated by the DSR.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

TmResponseTimeUpstream

Measurement ID
10002

Measurement Group
Diameter Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Connection ID)

Description
Average time (in milliseconds) from when routing forwards a Request message to an upstream peer to the time that an Answer response is received.

Collection Interval
5 min

Peg Condition
Time interval for each transaction starts when the DRL successfully queues a Request message to the DCL/RCL. Time interval for each transaction stops when the DRL receives an Answer response for the pending transaction associated with the forwarded Request message.

The connection measurement is associated with the connection the Request message is sent to.

Note: This measurement excludes transactions which are aborted due to a failure (e.g., timer PENDING-ANSWER-TIMER or PENDING-TRANSACTION-TIMER expiration or transport connection failure).

Measurement Scope
Server Group

Recovery

1. It is recommended to contact My Oracle Support for assistance if needed.

TxConnAnswerMsgs

Measurement ID
10154

Measurement Group
Diameter Egress Transaction, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of routable Answer messages successfully sent on the connection.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter Answer message is sent to the peer.

Measurement Scope
Server Group

Recovery

1. No action required.

TxConnRequestMsgs

Measurement ID
10153

Measurement Group
Diameter Egress Transaction, Diameter Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of routable Request messages successfully sent on the connection.

Collection Interval
5 min

Peg Condition
Pegged when a Diameter request message is sent to the peer.

Measurement Scope
Server Group

Recovery

1. No action required.

TxRequestSuccessAllMP

Measurement ID
10090

Measurement Group
Diameter Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Request messages successfully routed to a peer.

Collection Interval
5 min

Peg Condition
When the DSR successfully queues a Request message.

The connection measurement is associated with the connection to which the Request message was sent.

Measurement Scope
Server Group

Recovery

1. No action required.

Diameter Rerouting measurements

The Diameter Rerouting measurement report is a set of measurements which allows the user to evaluate the amount of message rerouting attempts which are occurring, the reasons for why message rerouting is occurring, and the success rate of message rerouting attempts.

MpRerouteToRequestRatio

Measurement ID
14014

Measurement Group
Diameter Rerouting

Measurement Type
Average

Measurement Dimension
Single

Description
Ratio of Request reroutes due to Answer Result-Code and/or Answer timeout to Total Requests routed by DSR.

Collection Interval
5 min

Peg Condition
The numerator of this measurement is pegged when request message reroute is triggered under these conditions:

- When DRL does not receive an answer from an upstream Peer Node within the PAT expiry.
- When DRL receives an Answer response from an upstream Peer Node and it finds a match in the Reroute on Answer table.

The denominator of this measurement is pegged under these scenarios:

- First attempt of Request routing
- First attempt of Message Copy Request routing

Measurement Scope
Site

Recovery

1. No action required.

RxRerouteAnswerRsp

Measurement ID
10054

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of valid Answer messages received from an upstream peer that were associated with a pending rerouted transaction.

Collection Interval
5 min

Peg Condition
When the DSR receives an Answer message event with a valid transport connection ID for which a pending transaction associated with a rerouted message is found. The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRerouteAnswerRspMp

Measurement ID
10095

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of valid Answer messages received from an upstream peer that were associated with a pending rerouted transaction.

Collection Interval
5 min

Peg Condition
When the DSR receives an Answer message event with a valid Transport Connection ID for which a pending transaction associated with a rerouted message is found. The connection measurement is associated with the connection from which the Answer message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

TxRerouteAnswerResponse

Measurement ID
10055

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of message rerouting attempts triggered by the receipt of an Answer response Result-Code value that is a candidate for message rerouting.

Collection Interval
5 min

Peg Condition
When the DSR receives an Answer response with a Result-Code value that is a candidate for message rerouting. The connection measurement is associated with the upstream connection from which the Answer response was received.

Measurement Scope
Server Group

Recovery

1. No action required.

TxRerouteAnswerTimeout

Measurement ID
10052

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of message rerouting attempts triggered by a timeout (PENDING-ANSWER-TIMER) on the Answer response.

Collection Interval
5 min

Peg Condition
When timer PENDING-ANSWER-TIMER expires and the DSR attempts to reroute a Request message.

Measurement Scope
Server Group

Recovery

1. If the user-configurable answer response timer is set too low it can cause the timer to expire before a Answer response is received. The user-configurable value is set from the **Diameter** > **Configuration** > **System Options** page.
2. It is recommended to contact My Oracle Support for assistance if needed.

TxRerouteAttempts

Measurement ID
10050

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Total number of message rerouting attempts.

Collection Interval
5 min

Peg Condition
When the DSR attempts to reroute a Request message routed via a Route List for various potential reasons:

- Transport connection fails
- PENDING-ANSWER-TIMER expires
- Answer response Result-Code plus application ID matches user-defined values for message rerouting

This measurement will be pegged when measurement TxRerouteConnFailure, TxRerouteAnswerTimeout, or TxRerouteAnswerResponse is pegged.

The connection measurement is associated with the upstream connection from which rerouting was triggered.

Measurement Scope

Recovery

1. If the user-configurable answer response timer is set too low it can cause the timer to expire before an Answer response is received. The user-configurable value is set from the **Diameter** > **Configuration** > **System Options** page.
2. Connection status can be monitored from the **Diameter** > **Maintenance** > **Connections** page.
3. It is recommended to contact My Oracle Support for assistance if needed.

TxRerouteConnFailure

Measurement ID
10051

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of message rerouting attempts triggered by a connection failure.

Collection Interval
5 min

Peg Condition
For each Request message rerouting attempt invoked by the receipt of a valid Connection Down event notification from the DSR.

Measurement Scope
Server Group

Recovery

1. Connection status can be monitored from the **Diameter** > **Maintenance** > **Connections** page.
2. It is recommended to contact My Oracle Support for assistance if needed.

TxRerouteSuccessSent

Measurement ID
10053

Measurement Group
Diameter Rerouting

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of message rerouting attempts that were successfully rerouted.

Collection Interval
5 min

Peg Condition
When the DSR successfully reroutes a Request message. The connection measurement is associated with the upstream connection from which rerouting was triggered.

Measurement Scope
Server Group

Recovery

1. No action required.

Link Exception measurements

The Link Exception measurement report contains measurements that provide information that is specific to links configured for the MP server.

EvLnkActAckTO

Measurement ID
9120

Measurement Group
Link Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of times the link timed out waiting for ASP-ACTIVE-ACK. An ASP-ACTIVE-ACK is sent by the SG in response to an ASP-ACTIVE message on the link. The link is not available for M3UA data signaling until the ASP-ACTIVE-ACK is received.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an ASP-ACTIVE has been sent for the link and the M3UA State Management ACK timer has expired, but no ASP-ACTIVE-ACK was received for the link.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. You can view Link status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Links**.
2. Check the event history log from the GUI main menu under **Alarms & Events** > **View History**. Look for Event ID 19229, which shows when the ASP-ACTIVE-ACK timeout occurs.

3. Verify that the far-end of the link on the SG is not undergoing maintenance.
4. Verify that the **State Management ACK Timer** period is not set too short.
5. Verify that the IP network between the MP server and the SG is performing up to expectations.
6. It is recommended to contact My Oracle Support for assistance if needed.

RxLnkUnsolInactAck

Measurement ID
9121

Measurement Group
Link Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of times an unsolicited ASP-INACTIVE-ACK was received on the link. ASP-INACTIVE-ACK may be sent unsolicited by the SG to indicate that the specified link is no longer able to process M3UA data signaling. The MP server will begin attempts to bring the link back into the signaling state matching its administrative state. For example, if the link is **Enabled**, the MP server will attempt to restore M3UA data signaling on the link by sending an ASP-ACTIVE and waiting for an ASP-ACTIVE-ACK.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an unsolicited ASP-INACTIVE-ACK is received on the link.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a zero value. A non-zero value means that the far-end of the link has stopped processing M3UA data. You can view Link status from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Links**.
2. Check the event history log from the GUI main menu under **Alarms & Events** > **View History**, looking for Event ID 19230. Event ID 19230 will show when the unsolicited ASP-INACTIVE-ACK was received.
3. Verify whether the far-end of the link is undergoing maintenance.
4. It is recommended to contact My Oracle Support for assistance if needed.

RxLnkM3uaERROR

Measurement ID
9123

Measurement Group
Link Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of times an M3UA ERROR message was received for the link. M3UA ERROR message are sent to indicate invalid M3UA signaling.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA ERROR message is received and that ERROR message can be attributed to a specific link (i.e., the ERROR message contains a valid routing context, or no routing context is needed).

Measurement Scope
NE, Server

Recovery

1. This measurement should have a value of zero. A non-zero value indicates a problem with the M3UA signaling sent by the MP server.
2. Look for Event ID 19235 from the GUI main menu under **Alarms & Events** > **View History**. **Event ID 19235** provides information on the reason for the receipt of the ERROR message.
3. If the ERROR reason in Event ID 19235 indicates a problem with routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. It is recommended to contact My Oracle Support for assistance if needed.

RxLnkInvalidM3ua

Measurement ID
9144

Measurement Group
Link Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of invalid M3UA messages received on the link. Invalid M3UA messages are messages that violate the M3UA protocol, but which can be attributed to a specific link (i.e., a valid routing context exists or no routing context is necessary).

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an invalid M3UA message is received for the link.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a value of zero. A non-zero value indicates a problem with the M3UA signaling received by the MP server.
2. Look for Event ID 19231 from the GUI main menu under **Alarms & Events** > **View History**. Event ID 19231 provides information on the reason the M3UA message was rejected.
3. If the ERROR reason in Event ID 19231 indicates a problem with the routing context (i.e., error code 0x19), verify that the MP server link set and the SG are configured to agree on the routing context values that each M3UA signaling link uses.
4. It is recommended to contact My Oracle Support for assistance if needed.

Link Performance measurements

The Link Performance measurement report contains measurements that provide performance information that is specific to links configured for the MP server.

Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are not counted in these measurements.

TxLnkMSU

Measurement ID
9113

Measurement Group
Link Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of MSUs sent on the link, including all M3UA messages, both DATA and non-DATA.

> **Note:** ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA message is sent on the link.

Measurement Scope
NE, Server

Recovery

1. No action required

RxLnkMSU

Measurement ID
9114

Measurement Group
Link Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of MSUs received on the link. MSUs includes all M3UA messages, both DATA and non-DATA. Note: ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA message is received on the link.

Measurement Scope
NE, Server

Recovery

1. No action required.

TxLnkMSUOctets

Measurement ID
9115

Measurement Group
Link Performance

Measurement Type
Arrayed (per link)

Measurement Dimension
Simple

Description
The number of MSU octets sent on the link, including all M3UA messages, both DATA and non-DATA.

> **Note:** ASPSM messages and some M3UA ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval
30 min

Peg Condition
This measurement is incremented by the number of octets in the MSU (not including SCTP, IP, or Ethernet headers) each time an M3UA message is sent on the link.

Measurement Scope
NE, Server

Recovery

1. No action required.

RxLnkMSUOctets

Measurement ID
9116

Measurement Group
Link Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link)

Description
The number of MSU octets received on the link – MSU octets includes all M3UA messages, both DATA and non-DATA. Note: ASPSM messages and some M3UA

ERROR messages cannot be mapped to a link and are therefore not counted in this measurement.

Collection Interval
30 min

Peg Condition
This measurement is incremented by the number of octets in the MSU (not including SCTP, IP, or Ethernet headers) each time an M3UA message is received on the link.

Measurement Scope
NE, Server

Recovery

1. No action required.

Link Set Performance measurements

The Link Set Performance measurement report contains measurements that provide performance information that is specific to link sets configured for the MP server.

TxLnkSetMSU

Measurement ID
9124

Measurement Group
Link Set Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link set)

Description
The number of MSUs sent on the link set , including all M3UA DATA messages sent on all links in the link set.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA DATA message is sent on a link in the link set.

Measurement Scope
NE, Server

Recovery

1. No action required.

RxLnkSetMSU

Measurement ID
9125

Measurement Group
Link Set Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link set)

Description
The number of MSUs sent on the link set, including all M3UA DATA messages received on all links in the link set.

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time an M3UA DATA message is received on a link in the link set.

Measurement Scope
NE, Server

Recovery

1. No action required.

TxLnkSetMSUOctets

Measurement ID
9126

Measurement Group
Link Set Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link set)

Description
The number of MSU octets sent on the link set, including all M3UA DATA octets sent on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.

Collection Interval
30 min

Peg Condition
This measurement is incremented by the number of octets in the M3UA DATA message each time an M3UA DATA message is sent on a link in the link set.

Measurement Scope
NE, Server

Recovery

1. No action required.

RxLnkSetMSUOctets

Measurement ID
9127

Measurement Group
Link Set Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per link set)

Description
The number of MSU octets received on the link set, including all M3UA DATA octets received on all links in the link set. Octets for SCTP, IP, and Ethernet headers are not included.

Collection Interval
30 min

Peg Condition
This measurement is incremented by the number of octets in the M3UA DATA message each time an M3UA DATA message is received on a link in the link set.

Measurement Scope
NE, Server

Recovery

1. No action required.

Link Set Usage measurements

The Link Set Usage measurement report contains measurements that provide usage information that is specific to link sets configured for the MP server.

TmM3RLLinksetUnavail

Measurement ID
9090

Measurement Group
Link Set Usage

Measurement Type
Duration

Measurement Dimension
Arrayed (by Linkset)

Description
Total time (in seconds) that all links in the link set were unavailable to M3RL during the measurement interval, regardless of whether the links were automatically or manually made unavailable.

Collection Interval
30 min

Peg Condition
M3RL must maintain an accurate time and measurement of the number of seconds during the collection period that the Link Set's state is **Unavailable**. This measurement is associated with the duration (in seconds) that Alarm 19202 - Link Set Unavailable (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted during the collection period.

Start of duration measurement for Link Set "X" criteria:

1. Alarm 19202 is asserted for Link Set "X."
2. Start of new collection period AND Alarm 19202 for Linkset "X" is already asserted (during a previous collection interval).

Stop of duration measurement for Link Set "X" criteria:

1. Alarm 19202 for Linkset "X" is cleared (i.e, Link Set becomes **Available**).
2. End of collection interval.

Measurement Scope

Recovery

1. This value provides a measure of the availability of a Link Set. No action required.

Link Usage measurements

The Link Usage measurement report contains measurements that provide usage information that is specific to links configured for the MP server.

TmLnkMOOS

Measurement ID
9117

Measurement Group
Link Usage

Measurement Type
Duration

Measurement Dimension
Arrayed (per link)

Description
The number of seconds the link is manual out of service during the reporting period. A link is manual out of service when the link is in the **Disabled** administrative state.

Collection Interval
Time is accumulated for this measurement when the link administrative state is set to **Disabled**.

> **Note:** The link is not considered to be manually out of service if the link is in the **Enabled** administrative state even if the association that hosts the link is manually out of service.

Peg Condition
30 min

Measurement Scope
NE, Server

Recovery

1. If a non-zero value in this field is unexpected (i.e., no link maintenance is known to have occurred), the link status can be viewed from the GUI under **SS7/Sigtran** > **Maintenance** > **Links**.
2. Also, look in the GUI main menu under **Alarms & Events** > **View History** in the event history for Event 19234 - Local link maintenance state change (refer to the *DSR Alarms and KPIs Reference* for details about this event). Event 19234 records each change in the link's administrative state. If the link was known to be under maintenance, this value represents the number of seconds during the reporting period that the link was in the **Disabled** administrative state.

TmLnkOOS

Measurement ID
9118

Measurement Group
Link Usage

Measurement Type
Duration

Measurement Dimension
Arrayed (per link)

Description
The number of seconds the link is out of service for any reason during the reporting period. A link may be out of service due to the following conditions:

- Maintenance activity – link is **Disabled** or link's association is **Disabled** or **Blocked**.
- Failure of the link to receive ASP-ACTIVE-ACK.

- Receipt of unsolicited ASP-INACTIVE-ACK from the SG.
- The link's association is not in the **Normal** status – failed to establish SCTP connection, failed to receive ASP-UP-ACK, received unsolicited ASP-DOWN-ACK

Collection Interval
30 min

Peg Condition
Time is accumulated for this measurement when the link status reason is not **Normal**.

Measurement Scope
NE, Server

Recovery

1. This measurement should have a value of zero. If the link or the link's association is known to be under maintenance, then a non-zero value in this measurement is expected.
2. Otherwise, the link status can be viewed from the GUI main menu under **SS7/ Sigtran** > **Maintenance** > **Links**.
3. Also look in the event history from the GUI main menu under **Alarms & Events** > **View History** for events related to this link or the link's association.
4. It is recommended to contact My Oracle Support for assistance if needed.

TmLnkAvailable

Measurement ID
9119

Measurement Group
Link Usage

Measurement Type
Duration

Measurement Dimension
Arrayed (per link)

Description
The number of seconds the link is in service during the reporting period. The link is considered to be in service if the link's status reason is **Normal**. An in-service link is available for M3UA DATA signaling.

Collection Interval
30 min

Peg Condition
Time is accumulated for this measurement when the link status reason is **Normal**.

Measurement Scope
NE, Server

Recovery

1. If all is well, this value should equal the length of the reporting period, meaning that the link was active for the entire reporting period. If the link-available time is not equal to the reporting period, it could be due to one of the following conditions:
   - Link maintenance. The measurements **TmLnkMOOS** and **TmLnkOOS** should have a non-zero values. See the actions for TmLnkMOOS.
   - Link failure. The measurement **TmLnkOOS** should have a non-zero value. See the actions forTmLnkOOS.
   - The link was added during the reporting period. The report indicates that the data is incomplete for the reporting period.
2. It is recommended to contact My Oracle Support for assistance if needed.

EvLnkManClose

Measurement ID
9145

Measurement Group
Link Usage

Measurement Type
Simple

Measurement Dimension

Description
The number of times a link was closed due to manual action. This count indicates the number of times that a link transitioned from ASP-ACTIVE to ASP-INACTIVE as a direct result of someone changing the link administrative state from **Enabled** to **Disabled**

Collection Interval
30 min

Peg Condition
This measurement is incremented by one each time the link administrative state is changed from **Enabled** to **Disabled**, causing a protocol state transition from ASP-ACTIVE to ASP-INACTIVE.

Measurement Scope
NE, Server

Recovery

1. If the link is known to be under maintenance, then no further action is necessary. If the link was not known to be under maintenance, then link status can be viewed from the GUI main menu under **SS7/Sigtran** > **Maintenance** > **Links**.
2. View the event history from the GUI main menu under **Alarms & Events** > **View History** looking for **Event ID 19234**. **Event ID 19234** shows the manual link state transitions and contains a time-stamp of when the change occurred.

3. The security logs from the GUI main menu under **Security Logs** can be searched using the time-stamp from the event history log to determine which login performed the manual state change on the link.
4. It is recommended to contact My Oracle Support for assistance if needed.

Message Copy measurements

The Diameter Application Server (DAS) measurements reflect the **Message Copy** performance. These measurements allow the user to monitor the amount of traffic being copied and the percentage of times that messages were successfully (or unsuccessfully) copied. Measurements such as the following are included in this group:

- Number of messages being copied
- Number of errors in transmitting those copies (i.e., retransmits)
- Number of times a copy transaction failed
- Tx and **Message Copy** queue utilization

DASCopyAnswerRx

Measurement ID
10065

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
The total number of DAS Copy Answers received.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time an Answer response is received from a DAS peer.

Measurement Scope
Server Group

Recovery

1. No action required.

   This measurement is an indication of the **Message Copy** response traffic load being processed by the MP.

DASCopyDiscarded

Measurement ID
10069

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total number of **Message Copy** failures because of any error (no Answer received, the result code in the Answer didn't match provisioning).

Collection Interval
5 min

Peg Condition
This measurement is incremented each time a DAS Copy fails for any reason. Some failure reasons include (but are not limited to): no answer from peer, Application ID not supported at the peer, result code in the Answer incorrect/doesn't match provisioning.

Measurement Scope
Server Group

Recovery

1. Verify proper routing to the intended DAS peer is configured and in service (route list is properly configured), Diameter application is selecting intended route list.
2. Verify intended DAS peer is properly configured to receive the intended traffic and traffic load.
3. Verify no network issues exist between the **MP** and intended DAS peer.
4. It is recommended to contact My Oracle Support for assistance.

DASCopyFailureMCCSNotProvisioned

Measurement ID
10089

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total amount of DAS Copy failures due to the copied message not finding a provisioned MCCS.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time the Copy Pending Transaction is discarded because the original message does not contain a valid MCCS, thus causing the copy action to fail.

Measurement Scope
Server Group

Recovery

1. Verify the MCCS configured with the trigger points and ensure proper provisioning.
2. If the problem persists, it is recommended to contact My Oracle Support.

DASCopyFailureMPCong

Measurement ID
10068

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total number of DAS Copy Failures because the **MP** was congested.

Collection Interval
5 min

Peg Condition
When the **MP** declares congestion (declared CL1-CL3), the **Message Copy** function is disabled. Original messages marked for copy and held as a Pending Transactions are not copied and increment this measurement. If the Copy has been sent to the DAS peer, the Copy transaction will be allowed to complete. If the Copy transaction fails, another measurement will be incremented.

Either the **MP** is receiving traffic in excess of its rated capacity or the intended DAS peer is not responding in a timely fashion.

Measurement Scope
Server Group

Recovery

1. Reduce traffic being received by the MP.
2. Verify there are no network issues between the **MP** and the intended DAS peer.
3. Ensure the intended DAS peer has sufficient capacity to process the traffic being directed to it by the MP
4. It is recommended to contact My Oracle Support for assistance.

DASCopyFailurePeerAppIdUnsup

Measurement ID
10059

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total amount of DAS Copy Failures because the Diameter Application Layer has specified a route list with no peer for the application ID in the message.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time the Copy Pending Transaction is discarded because a Diameter Request has been marked for copy by the application, but no connection in the provided Route List supports the Application ID in the request, causing the copy action to fail.

Measurement Scope
Server Group

Recovery

1. Verify the route list provisioning points to the intended DAS peer, and the intended DAS peer is responding with the desired Application ID.
2. It is recommended to contact My Oracle Support for assistance.

DASCopyFailureSizeExceeded

Measurement ID
10058

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total amount of DAS Copy failures due to the copied message size exceeding the maximum message size configured for the system.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time the Copy Pending Transaction is discarded because a the message being copied to the DAS exceeded the system set maximum message size, thus causing the copy action to fail.

Measurement Scope
Server Group

Recovery

1. Verify the maximum message size set system wide is sufficient for handling the messages being processed.
2. It is recommended to contact My Oracle Support for assistance.

DASCopyFailureRLNotProv

Measurement ID
10067

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total number of DAS Copy Failures because the route list is not provisioned.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time the Copy Pending Transaction fails because the indicated route list contained in the Diameter request does not match what has been provisioned as a system option or other provisioned route lists.

Measurement Scope
Server Group

Recovery

1. Review local provisioning that connections to intended DAS peer server(s) are in service and that no network issues exist in the path(s) to intended DAS peer server(s).
2. Review DAS peer provisioning to insure proper configuration.
3. It is recommended to contact My Oracle Support for assistance.

DASCopyRetransmits

Measurement ID
10056

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total number of DAS Copy retransmits.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time any Copied Message is retransmitted to a DAS peer because a qualified Diameter Answer response has not been received within the Pending Answer Timer's timeout value to complete the pending transaction.

Measurement Scope
Server Group

Recovery

1. Verify proper routing to the intended DAS peer is configured and in service (route list is properly configured), Diameter application is selecting intended route list.
2. Verify intended DAS peer is properly configured to receive the intended traffic and traffic load.
3. Verify no network issues exist between the **MP** and intended DAS peer.
4. It is recommended to contact My Oracle Support for assistance.

DASCopyRetransmitsExceeded

Measurement ID
10057

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total number of times the DAS Copy retransmits exceeded the configured max number of retransmits.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time a Copy Pending Transaction is discarded because the Copied Request has been retransmitted the configured number of times without receiving an Answer response from the DAS peer.

Measurement Scope
Server Group

Recovery

1. Verify proper routing to the intended DAS peer is configured and in service (route list is properly configured), Diameter application is selecting intended route list.
2. Verify intended DAS peer is properly configured to receive the intended traffic and traffic load.
3. Verify no network issues exist between the **MP** and intended DAS peer.
4. It is recommended to contact My Oracle Support for assistance.

DASCopyTx

Measurement ID
10064

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
The total number of DAS Copies forwarded.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time a **Message Copy** is transmitted to a DAS peer.

Measurement Scope
Server Group

Recovery

1. No action required.

   This measurement is an indication of the **Message Copy** traffic load being processed by the MP.

DASCopyValidAnswer

Measurement ID
10066

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
The total number of DAS Copy transactions completed (a Copy Pending Transaction has been paired with a qualified Answer from the DAS peer).

Collection Interval
5 min

Peg Condition
This measurement is incremented each time a Copy Pending Transaction is completed because a Diameter Copy Pending Transaction has been paired with a qualified Answer received from a DAS peer, completing the transaction.

Measurement Scope
Server Group

Recovery

1. Verify proper routing to the intended DAS peer is selected and in service.
2. desired answer result code is provisioned in the **Diameter** > **System Options**.
3. desired DAS peer is configured to return the answer result code provisioned in the **Diameter** > **System Options**.
4. It is recommended to contact My Oracle Support for assistance.

TxMsgCopyQueueAve

Measurement ID
10048

Measurement Group
DAS

Measurement Type
Average

Measurement Dimension
Single

Description
The average **Message Copy** Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
This measurement is pegged when a new **Message Copy** SysMetric sample is collected, then divided by the number of samples collected in the collection period.

Measurement Scope
Server Group

Recovery

1. No action required.

   This is a diagnostic indicator of the amount of traffic load being processed by the **Message Copy** feature.

TxMsgCopyQueueFullDiscard

Measurement ID
10084

Measurement Group
DAS

Measurement Type
Simple

Measurement Dimension
Single

Description
Total number of DAS Request messages discarded because the **Message Copy** queue was full.

Collection Interval
5 min

Peg Condition
This measurement is incremented each time a DAS Request is discarded because the **Message Copy** Tx queue was full, thus preventing a new DAS Request from being queued for transmit.

Measurement Scope
Server Group

Recovery

1. No action required.

   This is a diagnostic indicator of the amount of traffic load being processed by the **Message Copy** feature.

TxMsgCopyQueuePeak

Measurement ID
10047

Measurement Group
DAS

Measurement Type
Max

Measurement Dimension
Single

Description
The peak **Message Copy** Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
This measurement is pegged when a new **Message Copy** SysMetric sample is collected and the sample exceeds the previously saved peak for the collection period. When a new collection period is begun, the peak is reset to 0.

Measurement Scope
Server Group

Recovery

1. No action required.

   This is a diagnostic indicator of the amount of traffic load being processed by the **Message Copy** feature.

Message Priority measurements

The Message Priority measurement group contains measurements that provide information on message priority assigned to ingress Diameter messages. Measurements such as these are included in this group.

- Totals for the number of Request messages set to priority X when received from a peer.
- Totals for the number of Request messages set to priority X as a result of PRT processing.

RxMsgPri0ApplRule

Measurement ID
10039

Measurement Group
Message Priority

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of Request messages set to priority "0" as a result of ART processing

Collection Interval
5 min

Peg Condition
Each time DRL selects an application routing rule for routing a Request message, the rule action is set to "Route to Application", and a Message Priority of "0" is assigned to the application routing rule

Measurement Scope
Server Group

Recovery

1. No action required.

RxMsgPri0PeerRule

Measurement ID
10028

Measurement Group
Message Priority

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of Request messages set to priority “0” as a result of PRT processing.

Collection Interval
5 min

Peg Condition
Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to “Route to Peer”, and a Message Priority of “0” is assigned to the peer routing rule.

Measurement Scope
Server Group

Recovery

1. No action necessary.

RxMsgPri1ApplRule

Measurement ID
10045

Measurement Group
Message Priority

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of Request messages set to priority "1" as a result of ART processing

Collection Interval
5 min

Peg Condition
Each time DRL selects an application routing rule for routing a Request message, the rule action is set to "Route to Application", and a Message Priority of "1" is assigned to the application routing rule

Measurement Scope
Server Group

Recovery

1. No action required.

RxMsgPri1PeerRule

Measurement ID
10029

Measurement Group
Message Priority

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of Request messages set to priority “1” as a result of PRT processing.

Collection Interval
5 min

Peg Condition
Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to “Route to Peer”, and a Message Priority of “1” is assigned to the peer routing rule.

Measurement Scope
Server Group

Recovery

1. No action necessary.

RxMsgPri2AppIRule

Measurement ID
10049

Measurement Group
Message Priority

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of Request messages set to priority "2" as a result of ART processing

Collection Interval
5 min

Peg Condition
Each time DRL selects an application routing rule for routing a Request message, the rule action is set to "Route to Application", and a Message Priority of "2" is assigned to the application routing rule

Measurement Scope
Server Group

Recovery

1. No action required.

RxMsgPri2PeerRule

Measurement ID
10033

Measurement Group
Message Priority

Measurement Type
Simple

Measurement Dimension
Single

Description
Number of Request messages set to priority “2” as a result of PRT processing.

Collection Interval
5 min

Peg Condition
Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to “Route to Peer”, and a Message Priority of “2” is assigned to the peer routing rule.

Measurement Scope
Server Group

Recovery

1. No action necessary.

Message Processor (MP) Performance measurements

The **MP** Performance measurement report contains measurements that provide performance information for an **MP** server.

EvLongTimeoutPtrPoolAvg

Measurement ID
10295

Measurement Group
MP Performance

Measurement Type
Average

Measurement Dimension
Single

Description
The average Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The average of all Diameter Long Timeout PTR Buffer Pool utilization samples taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP, then a Diameter problem may exist that is causing excessive Long Timeout traffic to be delivered to the MP. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. If the problem persists, it is recommended to contact My Oracle Support.

EvLongTimeoutPtrPoolPeak

Measurement ID
10294

Measurement Group
MP Performance

Measurement Type
Max

Measurement Dimension
Single

Description
The peak Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.

A Long Timeout PTR is allocated for each Request message with a Pending Answer Timer value greater than 10 seconds that is forwarded to an upstream peer and is de-allocated when an Answer response is received and routed to a downstream peer. This measurement is useful for evaluating whether excessive traffic levels are being assigned to the Long Timeout pool. Assignment of traffic to this pool should be limited to Requests that are expected to have long response times.

Collection Interval
5 min

Peg Condition
The maximum Diameter Long Timeout PTR Buffer Pool utilization sample taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP, then a Diameter problem may exist that is causing excessive Long Timeout traffic to be delivered to the MP. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. If the problem persists, it is recommended to contact My Oracle Support.

EvMpCongestionLevel1Entered

Measurement ID
10285

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of times that the local DA-MP entered CPU congestion level 1.

Collection Interval
5 min

Peg Condition
Each time Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) transitions from "cleared" or asserted with severity "Info" to asserted with severity "Minor".

Measurement Scope
Server Group

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. DA-MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored 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. The ingress traffic rate of each DA-MP can be monitored 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. The alarm log be examined from **Main Menu** > **Status & Manage** > **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

EvMpCongestionLevel2Entered

Measurement ID
10287

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of times that the local DA-MP entered CPU congestion level 2.

Collection Interval
5 min

Peg Condition
Each time Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) transitions from "cleared" or asserted with severity "Info" or "Minor" to asserted with severity "Major".

Measurement Scope
Server Group

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. DA-MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored 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. The ingress traffic rate of each DA-MP can be monitored 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. The alarm log be examined from **Main Menu** > **Status & Manage** > **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

EvMpCongestionLevel3Entered

Measurement ID
10289

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of times that the local DA-MP entered CPU congestion level 3.

Collection Interval
5 min

Peg Condition
Each time Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) transitions from "cleared" or asserted with severity "Info", "Minor", or "Major" to asserted with severity "Critical".

Measurement Scope
Server Group

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. DA-MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored 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. The ingress traffic rate of each DA-MP can be monitored 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. The alarm log be examined from **Main Menu** > **Status & Manage** > **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

EvPtrListAvg

Measurement ID
10211

Measurement Group
MP Performance

Measurement Type
Average

Measurement Dimension
Single

Description
The average **Diameter** PTR Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The average of all Diameter PTR Buffer Pool utilization samples taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** when the ingress message rate and/or Diameter process CPU utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. It is recommended to contact My Oracle Support for assistance if needed.

EvPtrListPeak

Measurement ID
10210

Measurement Group
MP Performance

Measurement Type
Max

Measurement Dimension
Single

Description
The peak Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.

A PTR is allocated for each Request message that is forwarded to an upstream peer and is de-allocated when an Answer response is received and routed to a downstream

peer. This measurement is useful for evaluating whether persistent network or upstream server problems exist. In general, PTR buffers are engineered to match the processing capacity of the MP. If network or upstream server problems exist, delaying pending transactions in the MP, then PTRs (and associated messages/PDUs) will sit in internal Diameter queues.

Collection Interval
5 min

Peg Condition
The maximum Diameter PTR Buffer Pool utilization sample taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurements for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** when the ingress message rate and/or Diameter process CPU utilization measurements are below the recommended maximum engineered capacity of an MP, then a network (IP or Diameter) problem may exist. Looking at these measurements on a time of day basis may provide additional insight into potential network problems.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific software problem may exist (e.g., a buffer pool leak).
3. It is recommended to contact My Oracle Support for assistance if needed.

MpEvRadiusRoutedMsgs

Measurement ID
14074

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of ingress RADIUS messages processed by DRL, including Rerouting and Message Copy.

Collection Interval
5 min

Peg Condition
This measurement should be incremented as per the following conditions.

- Ingress RADIUS Request processing resulting in a Request being routed upstream (with or without local DSR application processing of the Request)
- Ingress RADIUS Response processing resulting in forwarding of Answer/Response downstream (with or without local DSR application processing of the Response)
- Ingress Request processing resulting in Answer message sent by DSR to originator (with or without local DSR application processing of the Request)
- Ingress RADIUS Request discarded due to validation error or overload
- Ingress RADIUS Response discarded due to validation error
- Initial copy and transmit of a RADIUS Request to a DAS
- Ingress RADIUS Response triggering reroute of the pending Request message (including Answers from DAS for copied RADIUS Requests)
- RADIUS Request reroute due to connection failure or Answer/Response timeout (including reroute of copied Requests to DAS for same reasons)
- Ingress Answer from a DAS terminated by DSR due to RADIUS Request copy completion or termination

Note: This is the functional equivalent to RoutingMsgs but for ingress RADIUS (only) messages. Measurement RoutingMsgs measures all ingress equivalent messages (Diameter and RADIUS).

Measurement Scope
Network

Recovery

1. No action required.

RxAnswerMsgQueueAvg

Measurement ID
10215

Measurement Group
MP Performance

Measurement Type
Average

Measurement Dimension
Single

Description
The average Answer Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The average of all Answer Message Queue utilization samples taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

RxAnswerMsgQueuePeak

Measurement ID
10214

Measurement Group
MP Performance

Measurement Type
Max

Measurement Dimension
Single

Description
The peak Answer Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The maximum Answer Message Queue utilization sample taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.

2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

RxRequestMsgQueueAvg

Measurement ID
10213

Measurement Group
MP Performance

Measurement Type
Average

Measurement Dimension
Single

Description
The average Request Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The average of all Request Message Queue utilization samples taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

RxRequestMsgQueuePeak

Measurement ID
10212

Measurement Group
MP Performance

Measurement Type
Max

Measurement Dimension
Single

Description
The peak Request Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The maximum Request Message Queue utilization sample taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an **MP** over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual **MP** is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist or a Diameter peer and/or DNS routing mis-configuration problem may exist.
3. It is recommended to contact My Oracle Support for assistance if needed.

TmMpCongestionLevel1

Measurement ID
10284

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The total time (in milliseconds) the local DA-MP was in CPU congestion level 1. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.

Collection Interval
5 min

Peg Condition
The "time interval" starts when one of the following conditions occur:

- A new "collection interval" for the measurement begins and Alarm 2220 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is already asserted with severity "Minor".
- Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted with severity "Minor" (onset of local DA-MP CPU congestion level 1 or abatement of local DA-MP CPU congestion levels 2 or 3).

The "time interval" stops when one of the following conditions occur:

- The "collection interval" for the measurement ends and Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is already asserted with severity "Minor".
- Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is no longer asserted with severity "Minor" (abatement of local DA-MP CPU congestion level 1 or onset of local DA-MP CPU congestion levels 2 or 3).

When the "time interval" completes, the time measured is added to the measurement value.

Measurement Scope
Server Group

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. DA-MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored 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. The ingress traffic rate of each DA-MP can be monitored 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. The alarm log be examined from **Main Menu** > **Status & Manage** > **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

TmMpCongestionLevel2

Measurement ID
10286

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The total time (in milliseconds) the local DA-MP was in CPU congestion level 2. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.

Collection Interval
5 min

Peg Condition
The "time interval" starts when one of the following conditions occur:

- A new "collection interval" for the measurement begins and Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is already asserted with severity "Major".
- Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted with severity "Major" (onset of local DA-MP CPU congestion level 2 or abatement of local DA-MP CPU congestion levels 3).

The "time interval" stops when one of the following conditions occur:

- The "collection interval" for the measurement ends and Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is already asserted with severity "Major".
- Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is no longer asserted with severity "Major" (abatement of local DA-MP CPU congestion level 2 or onset of local DA-MP CPU congestion levels 3).

When the "time interval" completes, the time measured is added to the measurement value.

Measurement Scope
Server Group

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. DA-MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored 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. The ingress traffic rate of each DA-MP can be monitored 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. The alarm log be examined from **Main Menu** > **Status & Manage** > **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

TmMpCongestionLevel3

Measurement ID
10288

Measurement Group
MP Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The total time (in milliseconds) the local DA-MP was in CPU congestion level 3. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.

Collection Interval
5 min

Peg Condition
The "time interval" starts when one of the following conditions occur:

- A new "collection interval" for the measurement begins and Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is already asserted with severity "Critical".
- Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted with severity "Critical" (onset of local DA-MP CPU congestion level 3).

The "time interval" stops when one of the following conditions occur:

- The "collection interval" for the measurement ends and Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is already asserted with severity "Critical".
- Alarm 22200 - Local MP Congestion (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is no longer asserted with severity "Critical" (abatement of local DA-MP CPU congestion level 3).

When the "time interval" completes, the time measured is added to the measurement value.

Measurement Scope
Server Group

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. DA-MP server status can be monitored from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each DA-MP can be monitored 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. The ingress traffic rate of each DA-MP can be monitored 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. The alarm log be examined from **Main Menu** > **Status & Manage** > **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

TxRerouteQueueAvg

Measurement ID
10219

Measurement Group
MP Performance

Measurement Type
Average

Measurement Dimension
Single

Description
The average Reroute Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The average of all Reroute Queue utilization samples taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer timeouts. The status of connections should be examined from the **Diameter** > **Maintenance** > **Connections** page.
2. If no additional congestion alarms are asserted, the routing answer 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, it is recommended to contact My Oracle Support.

TxRerouteQueuePeak

Measurement ID
10218

Measurement Group
MP Performance

Measurement Type
Max

Measurement Dimension
Single

Description
The peak Reroute Queue utilization (0-100%) measured during the collection interval.

Collection Interval
5 min

Peg Condition
The maximum Reroute Queue utilization sample taken during the collection interval.

Measurement Scope
Server Group

Recovery

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer timeouts. The status of connections should be examined from the **Diameter** > **Maintenance** > **Connections** page.
2. If no additional congestion alarms are asserted, the routing answer 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, it is recommended to contact My Oracle Support.

OAM.ALARM measurements

Table 5-1 OAM Alarm Measurements

Measurement Tag	Description	Collection Interval
Alarm.Crit	The number of critical alarms.	5 minutes
Alarm.Major	The number of major alarms.	5 minutes
Alarm.Minor	The number of minor alarms	5 minutes
Alarm.State	The alarm state.	5 minutes

OAM.SYSTEM measurements

Table 5-2 OAM System Measurements

Measurement Tag	Description	Collection Interval
System.CPU_UtilPct_Average	The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System.CPU_UtilPct_Peak	The peak CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System.Disk_UtilPct_Average	The average disk usage for the partition on which the COMCOL database resides.	5 minutes
System.Disk_UtilPct_Peak	The peak disk usage for the partition on which the COMCOL database resides.	5 minutes
System.RAM_UtilPct_Average	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 resources than provided by physical RAM, in which case, swapping will occur.	5 minutes
System.RAM_UtilPct_Peak	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.	5 minutes
System.ShMem_UtilPct_Average	The average shared memory usage as a percentage of the limit configured by shl.set.	5 minutes
System.ShMem_UtilPct_Peak	The peak shared memory usage as a percentage of the limit configured by shl.set.	5 minutes
System.SwapIn_Rate_Average	The average number of memory pages swapped in to memory from disk per second.	5 minutes
System.SwapIn_Rate_Peak	The peak number of memory pages swapped in to memory from disk per second.	5 minutes
System.SwapOut_Rate_Average	The average number of memory pages swapped out of memory from disk per second.	5 minutes

Table 5-2 (Cont.) OAM System Measurements

Measurement Tag	Description	Collection Interval
System.SwapOut_Rate_Peak	The peak number of memory pages swapped out of memory from disk per second.	5 minutes
System.Swap_UtilPct_Average	The average usage of swap space as a percentage of the total configured swap space.	5 minutes
System.Swap_UtilPct_Peak	The peak usage of swap space as a percentage of the total configured swap space.	5 minutes
System.CPU_CoreUtilPct_Average	The average CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.	5 minutes
System.CPU_CoreUtilPct_Peak	The peak CPU usage for each core. On an eight-core system, there will be eight sub-metrics showing the utilization of each core.	5 minutes

Peer Node Performance measurements

The Peer Node measurement group is a set of measurements that provide performance information that is specific to a Peer Node. These measurements will allow you to determine how many messages are successfully forwarded and received to/from each Peer Node. Measurements such as the following are included in this group.

EvPeerAvpDeleted

Measurement ID
14077

Measurement Group
Peer Node Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Node ID)

Description
The number of Diameter AVPs deleted by an AVP Removal List.

Collection Interval
5 min

Peg Condition
When DRL deletes one instance of an AVP from either a Request or Answer message based upon an AVP Removal List assigned to the Peer Node.

Measurement Scope
Site

Recovery

1. No action required.

RxPeerAnswers

Measurement ID
10078

Measurement Group
Peer Node Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Node ID)

Description
Number of routable Answer messages received from Peer-X.

Collection Interval
5 min

Peg Condition
When DRL receives an Answer message event from DCL with a valid Transport Connection ID owned by Peer-X.

Measurement Scope
Server Group

Recovery

1. No action required.

RxPeerRequests

Measurement ID
10077

Measurement Group
Peer Node Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Node ID)

Description
Number of routable Request messages received from Peer-X.

Collection Interval
5 min

Peg Condition
When DRL receives a Request message event from DCL with a valid Transport Connection ID owned by Peer-X.

Measurement Scope
Server Group

Recovery

1. No action required.

TxPeerAnswers

Measurement ID
10076

Measurement Group
Peer Node Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Node ID)

Description
Number of routable Answer messages sent to Peer-X.

Collection Interval
5 min

Peg Condition
When DRL successfully queues an Answer message for Peer-X to DCL.

Measurement Scope
Server Group

Recovery

1. No action required.

TxPeerRequests

Measurement ID
10075

Measurement Group
Peer Node Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Node ID)

Description
Number of routable Request messages sent to Peer-X.

Collection Interval
5 min

Peg Condition
When DRL successfully queues a Request message for Peer-X to DCL.

Measurement Scope
Server Group

Recovery

1. No action required.

Peer Routing Rules measurements

The Peer Routing Rules measurement report is a set of measurements associated with the usage of Peer Routing Rules. These measurements allow you to determine which Peer Routing Rules are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed using the Route List.

RxPrtSelected

Measurement ID
10079

Measurement Group
Peer Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (PRT ID)

Description
Number of times that a peer routing rule from PRT-X was selected for routing a Request message.

Collection Interval
5 min

Peg Condition
When the **DRL** selects a peer routing rule from PRT-X for routing a message.

Measurement Scope
Site

Recovery

1. No action required.

RxRuleDuplicatePriority

Measurement ID
10083

Measurement Group
Peer Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Routing Rule ID)

Description
The number of times that the Peer Routing Rule was selected for routing a message but another Peer Routing Rule had the same priority and was ignored.

Collection Interval
5 min

Peg Condition
When the DSR searches the Peer Routing Rules and finds more than one highest priority Peer Routing Rule with the same priority that matches the search criteria. The measurement is associated with the Peer Routing Rule that is selected for routing.

Measurement Scope
Server Group

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, it is recommended to contact My Oracle Support.

RxRuleFwdFailActionSendAns

Measurement ID
10082

Measurement Group
Peer Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Routing Rule ID)

Description
The number of times that the Peer Routing Rule was selected for routing a Request message and the message was not successfully routed because the Peer Routing Rule's action is Send Answer.

Collection Interval
5 min

Peg Condition
When the DSR selects a Peer Routing Rule to route a Request message and the Peer Routing Rule's action is Send Answer.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRuleFwdFailAll

Measurement ID
10081

Measurement Group
Peer Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Routing Rule ID)

Description
The number of times that the Peer Routing Rule was selected for routing a Request message and the message was not successfully routed for any reason other than "Send Answer" and "Abandon with No Answer".

Collection Interval
5 min

Peg Condition
When the DSR selects a Peer Routing Rule to route a Request message and one of the following conditions are met:

1. The Peer Routing Rule's action is Send Answer.

2. The Route List associated with the Peer Routing Rule has an Operational Status of Unavailable.
3. The DSR attempts to route the call but exhausts all routes associated with the Route List and sends an Answer response 3002 (DIAMETER_UNABLE_TO_DELIVER) .

The Route List measurement is associated with the Route List selected for routing.

Measurement Scope
Site

Recovery

1. If a Peer Routing Rule has been configured with the action Send Answer, then every time this Peer Routing Rule is selected for routing a message, this measurement will be incremented. A Peer Routing Rule's action can be viewed using the **Diameter** > **Configuration** > **Peer Routing Rules** page.
2. If a Peer Routing Rule has been configured with the action Route to Peer, then every time this Peer Routing Rule is selected for routing a message, the Route List associated with this Peer Routing Rule will be used for routing the message. The Peer Routing Rule's Route List can be viewed using the **Diameter** > **Configuration** > **Peer Routing Rules** page.

RxRuleSelected

Measurement ID
10080

Measurement Group
Peer Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Routing Rule ID)

Description
The number of times that the Peer Routing Rule was selected for routing a Request message.

Collection Interval
5 min

Peg Condition
When the DSR selects a Peer Routing Rule for routing a message.

Measurement Scope
Server Group

Recovery

1. No action required.

TxMsgPrtMarkedForCpy

Measurement ID
14013

Measurement Group
Peer Routing Rules

Measurement Type
Simple

Measurement Dimension
Arrayed (by Peer Routing Rule ID)

Description
The number of Request messages set to a valid MCCS and marked for Message Copy

Collection Interval
5 min

Peg Condition
Each time DRL selects a peer routing rule for routing a Request message, the rule action is set to "Route to Peer" and a MCCS is assigned to the peer routing rule.

Measurement Scope

Recovery

1. No action required.

Route List measurements

The Route List measurement report is a set of measurements associated with the usage of Route Lists. These measurements will allow the user to determine which Route Lists are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed using the Route List.

RxRouteListFailure

Measurement ID
10071

Measurement Group
Route List

Measurement Type
Simple

Measurement Dimension
Arrayed (by Route List ID)

Description
The number of times that a Route List was selected for routing a Request message and the DSR was unable to successfully route the message. There are several reasons why a message cannot be routed using a Route List:

- The Operational Status of the Route List is Unavailable
- The peers in the active Route Group do not support the Application ID in the Request message
- The Answer response timer is expiring for messages routed through the active Route Group
- Message loop detection is being detected for the peers in the active Route Group

Collection Interval
5 min

Peg Condition
When the DSR selects a Route List to route a Request message and either the Route List's Operational Status is Unavailable or the DSR attempts to route the call but exhausts all routesassociated with the Route List and sends an Answer response 3002 (DIAMETER_UNABLE_TO_DELIVER).

The Route List measurement is associated with the Route List selected for routing.

Measurement Scope
Server Group

Recovery

1. Check the Route List settings using the **Diameter** > **Configuration** > **Route Lists** page.
2. It is recommended to contact My Oracle Support for assistance if needed.

RxRouteListSelected

Measurement ID
10070

Measurement Group
Route List

Measurement Type
Simple

Measurement Dimension
Arrayed (by Route List ID)

Description
Number of times that Route List was selected for routing a Request message.

Collection Interval
5 min

Peg Condition
When the DSR selects a Route List for routing a message.

The Route List measurement is associated with the Route List selected for routing.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRouteListUnavailable

Measurement ID
10072

Measurement Group
Route List

Measurement Type
Simple

Measurement Dimension
Arrayed (by Route List ID)

Description
The number of Request messages from a downstream peer that were rejected by a Local Node because the selected Route List had an Operational Status of Unavailable.

Collection Interval
5 min

Peg Condition
Request message from a downstream peer is rejected by a Local Node because the selected Route List had an Operational Status of Unavailable. This occurs when the Route List was selected via a Peer Routing Rule or implicit routing but its Operational Status was Unavailable.

Measurement Scope
Server Group

Recovery

1. The operation status of the Route List should be verified using the **Diameter** > **Maintenance** > **Route Lists** page.
2. It is recommended to contact My Oracle Support for assistance if needed.

TmRouteListOutage

Measurement ID
10073

Measurement Group
Route List

Measurement Type
Simple

Measurement Dimension
Arrayed (by Route List ID)

Time (in seconds) that the Route List was unavailable. This will appear as an aggregate value retrieved from all DA-MPs in a Network Element.Description

Collection Interval
5 min

Peg Condition
The time duration interval starts when one of the following conditions occurs:

1. A new collection interval for the measurement begins and Alarm 22053 - Route List Unavailable (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted.
2. Alarm 22053 - Route List Unavailable (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted.

The time duration interval stops when one of the following conditions occurs:

1. The current collection interval for the measurement ends and Alarm 22053 - Route List Unavailable (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is asserted.
2. Alarm 22053 - Route List Unavailable (refer to the *DSR Alarms and KPIs Reference* for details about this alarm) is cleared.

When a time duration interval completes, the time measured is added to the total measurement value.

Measurement Scope

Recovery

1. The operation status of the Route List should be verified using the **Diameter** > **Maintenance** > **Route Lists** page.
2. It is recommended to contact My Oracle Support for assistance if needed.

Routing Usage measurements

The Routing Usage measurement report allows you to evaluate how ingress Request messages are being routed internally within the **Relay Agent**.

RxRoutedImplicitRealm

Measurement ID
14076

Measurement Group
Routing Usage

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages routed via Destination-Realm Implicit Routing.

Collection Interval
5 min

Peg Condition
The request message is routed using Destination-Realm Implicit Routing.

The "connection measurement" is associated with the Connection from whom the Request message was received.

Measurement Scope
Site

Recovery

1. No action required.

RxRoutedIntraMPAttempt

Measurement ID
10063

Measurement Group
Routing Usage

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of attempts to route an ingress request message via intra-MP routing.

Collection Interval
5 min

Peg Condition
When the DSR selects a transport connection controlled by the local MP and successfully queues the Request message on the local message queue. The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRoutedPeerDirect

Measurement ID
10061

Measurement Group
Routing Usage

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages implicitly routed directly to a peer.

Collection Interval
5 min

Peg Condition
When the DSR does not find a Peer Routing Rule that matches message content, the Destination-Host AVP is present and its value matches a FQDN of a peer, and the peer is available for egress routing. The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRoutedPeerRouteList

Measurement ID
10062

Measurement Group
Routing Usage

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages implicitly routed to a peer via its alternate implicit route.

Collection Interval
5 min

Peg Condition
When the DSR does not find a Peer Routing Rule that matches message content, the Destination-Host AVP is present and its value matches a FQDN of a peer, the peer is Unavailable for egress routing, and the user-defined alternate implicit route for the peer contains a valid Route List. The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

RxRoutedPrt

Measurement ID
10060

Measurement Group
Routing Usage

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of Request messages routed using Peer Routing Rules.

Collection Interval
5 min

Peg Condition
When the DSR selects the highest priority Peer Routing Rule which matches message content. The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope
Server Group

Recovery

1. No action required.

SBR Session Exception measurements

The Session Binding Repository (SBR) Session Exception measurement report contains measurements that provide performance information specific to the SBR Session Database.

SbrCreateSessDbErr

Measurement ID
10850

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of errors creating a session record.

Collection Interval
5 min

Peg Condition
This peg is updated whenever there is an error in creating a session record.

Measurement Scope
All

Recovery

1. No action necessary.

SbrRefreshSessDbErr

Measurement ID
10851

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of errors refreshing a session record.

Collection Interval
5 min

Peg Condition
This peg is updated whenever there is an error in refreshing a session record.

Measurement Scope
All

Recovery

1. No action necessary.

SbrRemSessDbErr

Measurement ID
10852

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of errors terminating a session record.

Collection Interval
5 min

Peg Condition
This peg is updated whenever there is an error in terminating a session record.

Measurement Scope
All

Recovery

1. No action necessary.

SbrFindSessDbErr

Measurement ID
10879

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of errors when encountered for finding a session record.

Collection Interval
5 min

Peg Condition
This peg is updated whenever there is an error in finding a session record.

Measurement Scope
All

Recovery

1. No action necessary.

SbrRemSessRarAttempts

Measurement ID
11301

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of sessions removed as a result of no response being received in 8 consecutive attempts to query the policy client for existence of the session.

Collection Interval
5 min

Peg Condition
This peg is incremented by one each time a session is removed due to lack of response after the maximum number of attempts to query the policy client have been attempted.

Measurement Scope
Network

Recovery

1. A non-zero value in this field may indicate that a policy client has become inaccessible after creating Diameter sessions on the Policy DRA.
2. If a policy client was purposely removed from service, please disregard this measurement.

SbrCreateOcSessionDbErr

Measurement ID
11387

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Online Charging session creation errors.

Collection Interval
5 min

Peg Condition
Each time a failure is encountered in creating an Online Charging Session record in the SBR Session database. Online Charging Session record failures include:

- Online Charging Session record already exists (i.e. retransmission)
- Database Access Failure

Measurement Scope
All

Recovery

1. No action necessary.

SbrFindOcSessionDbErr

Measurement ID
11388

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Online Charging session query errors.

Collection Interval
5 min

Peg Condition
Each time a failure is encountered in finding an Online Charging Session record in the SBR Session database.

Measurement Scope
All

Recovery

1. No action necessary.

SbrOcSessionNotFound

Measurement ID
11389

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Online Charging sessions not found.

Collection Interval
5 min

Peg Condition
Each time an Online Charging session record is not found in the SBR Session database.

Measurement Scope
All

Recovery

1. No action necessary.

SbrRefreshOcSessionDbErr

Measurement ID
11390

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Online Charging session refresh errors.

Collection Interval
5 min

Peg Condition
Each time there is a failure in refreshing an Online Charging session record in the SBR Session database.

Measurement Scope
All

Recovery

1. No action necessary.

SbrRemoveOcSessionDbErr

Measurement ID
11391

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of Online Charging session removal errors.

Collection Interval
5 min

Peg Condition
Each time there is a failure in deleting an Online Charging Session record from the SBR Session database.

Measurement Scope
All

Recovery

1. No action necessary.

TxPendingRarDeletedExceedMax

Measurement ID
12158

Measurement Group
SBR Session Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (by Query, Release, and Total)

Description
The number of pending RARs (Query or Release) that have been removed due to exceeding the maximum send attempts allowed per Query or Release RAR.

Collection Interval
5 min

Peg Condition
Each time a RAR entry in the queue/table is removed for exceeding the maximum attempts value. This measurement is incremented by one for each Query or Release RAR entry removed due to exceeding the maximum Send Attempts per Query or Release RAR value.

Measurement Scope
All

Recovery

1. Modify the "Maximum Attempts Per Query RAR" or "Maximum Attempts Per Release RAR" in **Policy and Charging** > **Configuration** > **Policy DRA** > **Network-Wide Options**.

Transport Exception measurements

The Transport Exception measurement group contains measurements that provide information about exceptions and unexpected events related to the Transport Manager.

RxTrFarEndClose

Measurement ID
9400

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the far end closed the SCTP connection

Collection Interval
30 min

Peg Condition
Each time the far-end of the association closes the association by sending either SHUTDOWN or ABORT

Measurement Scope
NE, Server

Recovery

1. If the closing of the association was expected, no further action is necessary - the association will be recovered as soon as the far-end is ready to connect again.

2. If the closing of the association was not expected:
   a. Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.
   b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** Event 19404 - Far-end closed the Transport to determine exactly when the far-end closed the association.
   c. Look for other events for the association or MP server in the event history.
   d. Verify that IP connectivity still exists between the MP server and the SG.
   e. Verify whether the far-end of the association is undergoing maintenance.

EvTrManClose

Measurement ID
9401

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the Transport was manually closed. This includes manual changes of the transport administrative state that cause the transport to transition from APP-UP to Disabled.

Collection Interval
30 min

Peg Condition
Each time a manual change is made to the transport administrative state from Enabled to Blocked or from Enabled to Disabled, causing the transport to transition our of APP-UP protocol state.

Note: This condition has a special meaning for SS7/M3UA where it is linked with ASP-UP.

Measurement Scope
NE, Server

Recovery

1. If the transport is known to be under maintenance, then no further action is necessary.
2. If the closing of the association was not expected:

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

b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** Event 19406 - Local Transport maintenance state change, which shows the manual transport state transitions and contains a time-stamp of when the change occurred.

c. The security logs at **Main Menu** > **Log Files** > **Security Logs History** can be searched using the time-stamp from the event history log to determine which login performed the manual state change on the association.

d. It is recommended to contact My Oracle Support for assistance if needed.

EvTrNoRespClose

Measurement ID
9402

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the transport was closed due to lack of response from the far end, including lack of response to any signaling sent on the transport.

Collection Interval
30 min

Peg Condition
Each time an established Transport is closed by the MP server due to lack of response at the SCTP level from the far-end of the association.

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. If non-zero, the association has been closed due to lack of response from the far-end. The MP server will begin periodic attempts to reconnect to the SG.
2. Otherwise:
   a. Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.
   b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** Event 19405 - Transport closed due to a lack of response (refer to the *DSR Alarms and KPIs Reference* for details about this event.

c. Verify IP connectivity between the MP server and the SG.

d. Determine if the far-end of the association is congested, possibly causing slow response times on the association.

e. Check the IP network between the MP server and the SG for excessive retransmissions.

f. It is recommended to contact My Oracle Support for assistance if needed.

EvTrCnxFail

Measurement ID
9404

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description

- The number of times the SCTP connection attempt failed on the transport. This includes only unsuccessful attempts to connect/accept SCTP connections. It does not include failure of established connections.
- The number of times open attempt on UDP socket in Listen Mode failed on the Transport.

Collection Interval
30 min

Peg Condition

- Each time an SCTP connect attempt fails
- Each time an UDP open attempt in Listen mode fails
- Each time an SCTP open attempt in Listen mode fails

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Peer IP Address at least once and failed to establish the SCTP connection.
2. Otherwise:
   a. Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.

b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** Event 19402 - Failed to connect Transport, which provides more details as to the actual cause of the failure.

c. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**.

d. Verify that the remote port configured at **Main Menu** > **Transport Manager** > **Configuration** > **Transport** for the association correctly identifies the port that the Adjacent Node is listening on for SCTP connections.

e. Verify the IP network connectivity between the MP server and the Adjacent Node.

f. If the SG must be configured to connect to the MP server's IP address and port, verify that the SG configuration matches the association configuration at **Main Menu** > **Transport Manager** > **Configuration** > **Transport**.

g. It is recommended to contact My Oracle Support for assistance if needed.

TxTrSendFail

Measurement ID
9405

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the SCTP/UDP send failed for signaling on the transport. This includes sending of any messages on an established transport or UDP socket.

Collection Interval
30 min

Peg Condition
Each time an attempt to send signaling DATA fails for any reason and the information being sent cannot be mapped to a specific transport

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. A non-zero value indicates that an attempt to send a message to the far-end on this Transport has failed. Normally this happens if the far-end cannot keep up with the rate of messages being sent from all links on the association.

2. Otherwise:

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

   b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** Event 19407 - Failed to send Transport DATA Message, which gives more information about exactly what caused the failure to send.

   c. Verify that the IP network between the MP server and the Adjacent Node is functioning as expected.

   d. It is recommended to contact My Oracle Support for assistance if needed.

RxTrRecvFailed

Measurement ID
9406

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times an SCTP/UDP receive attempt failed on the transport. Failure to receive message via SCTP may result in a message being discarded

Collection Interval
30 min

Peg Condition
Each time an SCTP receive fails when the far-end attempted to send data, but the data cannot be received due to an invalid message length

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. A non-zero value indicates that the far-end is sending data that is malformed.

2. Otherwise:

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

   b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** Event 19403 - received malformed SCTP message (invalid length), which gives more information about exactly what caused the failure.

   c. Try to bring the sockets back into alignment by manually Disabling and Enabling the Transport.

d. It is recommended to contact My Oracle Support for assistance if needed.

EvTrSockInitFail

Measurement ID
9407

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of times the socket initialization failed.

Collection Interval
30 min

Peg Condition
Each time one or more socket options cannot be set according to the settings in the transport's configuration set

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. A non-zero value indicates some problem with association setup prior to attempting to connect the association.
2. If this issue occurs, look in **Main Menu** > **Alarms & Events** > **View History** for Event 19401 - Failed to configure Transport, which provides details about exactly what part of the configuration failed.
3. It is recommended to contact My Oracle Support for assistance if needed.

TmSingleTransQueueFull

Measurement ID
9415

Measurement Group
Transport Exception

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of egress messages that were discarded because the single Transport Writer Queue was full.

Collection Interval
30 min

Peg Condition
Check whether the single peers transmit data queue limit has reached its max limit (1000). If max limit is reached or exceeded then peg the measurement and discard the low priority events.

Measurement Scope
NE, Server

Recovery

1. This measurements indicates that the Transport is backed up and there could be messages that will get discarded. If it's above the defined critical threshold, it results in generating Alarm 19408 - Single Transport Egress-Queue Utilization (refer to the *DSR Alarms and KPIs Reference* for details about this alarm).
2. The percent utilization of the MP's Transport Writer Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization, all new egress messages from the Transport will be discarded.

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

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

3. It is recommended to contact My Oracle Support for assistance if needed.

EvSctpAdjPToDwn

Measurement ID
9424

Measurement Group
Transport Exception

Measurement Type
Max

Measurement Dimension
Arrayed (per Transport)

Description
The number of times a configured IP Address of an Adjacent Node goes from Available to Unavailable.

Collection Interval
30 min

Peg Condition
Each time reachability to a configured IP address of an Adjacent Node is lost, indicating a fault in the path to that address was detected.

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. A non-zero value indicates a path fault to that address was detected.
2. Otherwise:
   a. Check the event history log at **Main Menu** > **Alarms & Events** > **View History**, looking for Event 19409 - Message Rejected by ACL Filtering which provide more details as to the actual cause of the failure.
   b. Verify the Adjacent Node that represents the far-end of the association is configured with the correct address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**.
   c. Verify the IP network connectivity between the MP server and the Adjacent Node's IP address using a ping or traceroute command
3. It is recommended to contact My Oracle Support for assistance if needed.

EvSctpTransRej

Measurement ID
9425

Measurement Group
Transport Exception

Measurement Type
Max

Measurement Dimension
Arrayed (per Transport)

Description
The number of times SCTP Transport has been rejected due to remote IP addresses validation failure based on SCTP Multihoming mode. This is valid only for SCTP Transports.

Collection Interval
30 min

Peg Condition
Each time the association has been rejected due to IP address validation failure in the SCTP INITs/INIT-ACKs transmitted by the Adjacent Node.

Measurement Scope
NE, Server

Recovery

1.

2. If all is well, this measurement should have a zero value. A non-zero value indicates that the Adjacent Node has attempted to connect to the Peer IP Address at least once and but the connection attempt was rejected because the IP addresses advertised by the Adjacent Node failed validation.

3. Otherwise:

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

   b. Check the event history log at **Main Menu** > **Alarms & Events** > **View History**, looking for Events 19411 - SCTP Transport closed due to failure of multihoming validation or 19412 - SCTP Transport Transport Configuration Mismatch which provide more details as to the actual cause of the failure.

   c. Verify that the SCTP validation mode is as desired.

   d. Verify that the Adjacent Node that represents the far-end of the association is configured with the correct address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**.

   e. Verify that the remote port configured at **Main Menu** > **Transport Manager** > **Configuration** > **Transport** for the association correctly identifies the port that the Adjacent node is listening on for SCTOp connections.

   f. It is recommended to contact My Oracle Support for assistance if needed.

Transport Usage measurements

The Transport Usage measurement group contains measurements that provide information about the usage of the Transport Manager.

EvTrCnxSuccess

Measurement ID
9403

Measurement Group
Transport Usage

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description

- The number of times the SCTP connection was successfully established on the transport.
- The number of times the UDP socket in Listen Mode was opened successfully on the transport.

Collection Interval
30 min

Peg Condition

- Each time the SCTP association reaches the APP-UP protocol state (i.e. the connection is successfully ESTABLISHED)
- Each time the UDP socket in Listen Mode was opened successfully

Measurement Scope
NE, Server

Recovery

1. If the association is expected to have connected during the measurement reporting interval, no action is necessary.
2. Otherwise:
   a. Transport status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.
   b. Look in the event history at **Main Menu** > **Alarms & Events** > **View History** events related to the association or the MP server to determine what may have caused the Transport to fail.
   c. It is recommended to contact My Oracle Support for assistance if needed.

TmTrEnaNotUp

Measurement ID
9410

Measurement Group
Transport Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (per Transport)

Description
The number of seconds during the reporting interval during which the transport was in the Enabled administrative state but was not in APP-UP protocol state. When the transport is Enabled, the desired protocol state is APP-UP. This measurement indicates the amount of time during the reporting interval for which the association was not in the desired protocol state.

Collection Interval
30 min

Peg Condition
Time shall be accumulated for this measurement during the collection interval when all of the following are true:

- the association is in the ENABLED administrative state
- the association is not in the ASP-UP protocol state for M3UA and APP-UP for other Plugins

Measurement Scope
NE, Server

Recovery

1. If all is well, this measurement should have a zero value. A non-zero value indicates that the MP server has attempted to connect to the Peer IP Address at least once and failed to establish the SCTP connection.
2. Otherwise:
   a. Association status can be viewed at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.
   b. Verify that the Adjacent server that represents the far-end of the association is configured with the correct IP address at **Main Menu** > **Transport Manager** > **Configuration** > **Adjacent Node**.
   c. Verify that the remote port configured at **Main Menu** > **Transport Manager** > **Configuration** > **Transport** for the association correctly identifies the port that the SG is listening on for SCTP connections.
   d. Verify the IP network connectivity between the MP server and the SG.
   e. If the Adjacent Node must be configured to connect to the MP server's IP address and port, verify that the Adjacent Node configuration matches the association configuration at **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.
   f. It is recommended to contact My Oracle Support for assistance if needed.

RxTmSctpBufAvg

Measurement ID
9411

Measurement Group
Transport Usage

Measurement Type
Average

Measurement Dimension
Arrayed (per Transport)

Description
The Average Value of the number of bytes in SCTP RX Window

Collection Interval
5 min

Peg Condition
Every Second, retrieve the Rx socket buffer occupancy by using the "getsockopt" functions and then calculates and peg the Average buffer occupancy, during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation.

Measurement Scope
NE, Server

Recovery

1. No action required. This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface.

RxTmSctpBufPeak

Measurement ID
9412

Measurement Group
Transport Usage

Measurement Type
Max

Measurement Dimension
Arrayed (per Transport)

Description
The Peak Value of the number of bytes in SCTP RX Window

Collection Interval
5 min

Peg Condition
Every Second, retrieve the Rx socket buffer occupancy by using the "getsockopt" functions and then calculates and peg the Maximum buffer occupancy during the last 5 min window. To calculate the current RX Buffer Occupancy, we subtract the number of unused bytes in the buffer from the initial default RX buffer size set during setsockopt at the time of socket creation.

Measurement Scope

Recovery

1. No action required. This is debug statistical information retrieved from getsockopt (SO_RCVBUF) interface.

Transport Performance measurements

The Transport Performance measurement group contains measurements that provide information about performance related measurements for the Transport Manager.

TxTrOctets

Measurement ID
9408

Measurement Group
Transport Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Transport)

Description
The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers

Collection Interval
30 min

Peg Condition
Each time a DATA/non-DATA message is successfully sent on the transport (incremented by the number of octets in the message)

Measurement Scope
NE, Server

Recovery

1. No action required. This measurement indicates the level of signaling octets that have been sent over the association during the reporting interval.

RxTrOctets

Measurement ID
9409

Measurement Group
Transport Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Transport)

Description
The number of octets sent on the SCTP/UDP Transport. It does not include SCTP, UDP, IP, or Ethernet headers

Collection Interval
30 min

Peg Condition
Each time a DATA/non-DATA message is successfully received on the transport (incremented by the number of octets in the message)

Measurement Scope
NE, Server

Recovery

1. No action required. This measurement indicates the level of signaling octets that have been sent over the association during the reporting interval.

TmSingleTransQueuePeak

Measurement ID
9413

Measurement Group
Transport Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by Transport)

Description
The peak single Transport Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec)

Collection Interval
5 min

Peg Condition
Transport's Queue is registered as a Stack Resource, StackResourceManager thread monitors and updates the maximum Transport Queue utilization sample taken during the collection interval for affected Transport

Measurement Scope
NE, Server

Recovery

1. Transport single queue utilization depicts the SCTP or UDP Transport Writer Queues utilization. This is a measure of how fast the Transport queue is being processed. It indicates the maximum depth of queue over the monitored interval. It

is primarily intended to assist in evaluating the needed for additional MP processing capacity at a Network Element.

2. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.

3. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

   a. An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being received form the network.

   b. The SCTP Association Writer process may be experiencing a problem preventing it from processing events from its event queue. The alarm log should be examined from **Main Menu** > **Alarms & Events**.

   c. 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 & Control** > **Server Status**.

   d. The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.

   e. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Main Menu** > **Status & Control** > **KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

5. It is recommended to contact My Oracle Support for assistance if needed.

TmSingleTransQueueAvg

Measurement ID
9414

Measurement Group
Transport Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by Transport)

Description
The average single Transport (SCTP/UDP) Writer Queue utilization (0-100%) measured during the collection interval (averaged over 2 sec)

Collection Interval
5 min

Peg Condition
Transport's Queue is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport

Measurement Scope
NE, Server

Recovery

1. This is a measure of how fast the Transport queue is being processed. It indicates the Average depth of queue over the monitored interval. It is primarily intended to assist in evaluating the need for additional MP processing capacity at a Network Element.
2. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased
3. If the peak and average for an individual MP are significantly different than other MPs in the same Network Element, then an MP-specific hardware, software, or configuration problem may exist
4. It is recommended to contact My Oracle Support for assistance if needed.

SctpTransPeerCWNDPeak

Measurement ID
9416

Measurement Group
Transport Performance

Measurement Type
Max

Measurement Dimension
Arrayed (per Transport)

Description
The peak value of congestion window size recorded for the peer of a SCTP transport during the collection interval

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS), It indicates Peak of congestion window recorded for the peer address.

SctpTransPeerCWNDAvg

Measurement ID
9417

Measurement Group
Transport Exception

Measurement Type
Average

Measurement Dimension
Arrayed (per Transport)

Description
The average of congestion window size recorded for the peer of a SCTP transport during the collection interval.

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS); It indicates Average of congestion window recorded for the peer address.

SctpTransPeerSRTTPeak

Measurement ID
9418

Measurement Group
Transport Performance

Measurement Type
Max

Measurement Dimension
Arrayed (per Transport)

Description
The peak value of smoothed round trip time for the SCTP Transport address during the collection interval

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransPeerSRTTAvg

Measurement ID
9419

Measurement Group
Transport Performance

Measurement Type
Average

Measurement Dimension
Arrayed (per Transport)

Description
The average value of smoothed round trip time for the SCTP Transport address during the collection interval.

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransUnAckedDataPeak

Measurement ID
9420

Measurement Group
Transport Performance

Measurement Type
Max

Measurement Dimension
Arrayed (per Transport)

Description
The peak number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval.

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Peak value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API.

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransUnAckedDataAvg

Measurement ID
9421

Measurement Group
Transport Performance

Measurement Type
Average

Measurement Dimension
Arrayed (per Transport)

Description
The average number of unacknowledged DATA chunks pending for the peer of a SCTP Transport address during the collection interval

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransRTOPeak

Measurement ID
9422

Measurement Group
Transport Performance

Measurement Type
Average

Measurement Dimension
Arrayed (per Transport)

Description
The average value of retransmission timeout in use for the SCTP Transport address

Collection Interval
30

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

SctpTransRTOAvg

Measurement ID
9423

Measurement Group
Transport Performance

Measurement Type
Average

Measurement Dimension
Arrayed (per Transport)

Description
The average value of retransmission timeout in use for the SCTP Transport address

Collection Interval
30 min

Peg Condition
This Metric is registered as a Stack Resource, StackResourceManager thread monitors and updates the metric Average value for affected Transport. SCTP status information will be retrieved from socket option "SCTP_STATUS" through sctp_opt_info API

Measurement Scope
NE, Server

Recovery

1. This is debug information, which is retrieved from sctp socket option (SCTP_STATUS).

Topology Hiding Performance measurements

The Topology Hiding Performance measurement report contains measurements providing information on the number of messages that the various topology hiding methods were applied.

TxPathTopology

Measurement ID
14020

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of messages given path topology hiding treatment on messages routed to an Untrusted Network

Collection Interval
5 min

Peg Condition
Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTH and ATH respectively

Measurement Scope
Site

Recovery

1. No action required.

RxPathTopology

Measurement ID
14021

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of messages given path topology hiding treatment on messages received from an Untrusted Network

Collection Interval
5 min

Peg Condition
Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTR and ATR respectively

Measurement Scope
Site

Recovery

1. No action required.

EvHssTopology

Measurement ID
14022

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of messages given S6a/S6d HSS topology hiding treatment

Collection Interval
5 min

Peg Condition
Each time S6a/S6d HSS TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR

> **Note:** If S6a/S6d HSS TH treatment is applied to more than one AVP in a message, the counter is only incremented once

Measurement Scope
Site

Recovery

1. No action required.

EvMmeTopology

Measurement ID
14023

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
Number of messages given MME/SGSN topology hiding treatment

Collection Interval
5 min

Peg Condition
Each time MME/SGSN TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR

> **Note:** If MME/SGSN TH treatment is applied to more than one AVP in a message, the counter is only incremented once

Measurement Scope
Site

Recovery

1. No action required.

EvMmeTopologyException

Measurement ID
14029

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of messages given exception treatment while applying MME/SGSN topology hiding treatment

Collection Interval
5 min

Peg Condition
When MME/SGSN TH exception treatment is applied to either a Request or Answer message at TH trigger points RTH and ATH

Measurement Scope
Site

Recovery

1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set

EvHssTopologyException

Measurement ID
14031

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment

Collection Interval
5 min

Peg Condition
When S6a/S6d HSS TH exception treatment is applied to a Request message at TH trigger point RTH

Measurement Scope
Site

Recovery

1. Check the HSS Vendor and request the vendor to be RFC 6733 Compliant

EvPcrfTopology

Measurement ID
14034

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of messages given S9 PCRF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 PCRF TH treatment is applied to either a Request or Answer message TH trigger points RTH, RTR, ATH, and ATR

Measurement Scope
Site

Recovery

1. No action required.

EvPcrfTopologyMp

Measurement ID
14035

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given S9 PCRF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 PCRF TH treatment is applied to either a Request or Answer message TH trigger points RTH, RTR, ATH, and ATR

Measurement Scope
Site

Recovery

1. No action required.

EvPcrfTopologyExceptionMp

Measurement ID
14036

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given exception treatment while applying S9 PCRF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 PCRF TH treatment is applied to either a Request or Answer message at RTH, RTR, or ATH trigger points and "PCRF Actual Name Not Found" Action is invoked

Measurement Scope
Site

Recovery

1. Check with the PCRF Vendor and request them to be RFC 6733 Compliant if the format of the Session-ID AVP is not RFC 6733 compliant.
2. Check the configuration of TH Host Names and ensure that all PCRF host names to hidden are present in the S9 PCRF TH Configuration Set

EvPcrfTopologyException

Measurement ID
14037

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of messages given exception treatment while applying S9 PCRF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 PCRF TH treatment is applied to either a Request or Answer message at RTH, RTR, or ATH trigger points and "PCRF Actual Name Not Found" Action is invoked

Measurement Scope
Site

Recovery

1. Check with the PCRF Vendor and request them to be RFC 6733 Compliant if the format of the Session-ID AVP is not RFC 6733 compliant.
2. Check the configuration of TH Host Names and ensure that all PCRF host names to hidden are present in the S9 PCRF TH Configuration Set

EvAfTopology

Measurement ID
14038

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Diameter Connection ID)

Description
The number of messages given S9 AF/pCSCF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 AF/pCSCF TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR

> **Note:** If S9 AF/pCSCF TH treatment is applied to more than one AVP in a message, the counter is only incremented once

Measurement Scope
Site

Recovery

1. No action required.

EvAfTopologyMp

Measurement ID
14039

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given S9 AF/pCSCF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 AF/pCSCF TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, ATH, and ATR

> **Note:** If S9 AF/pCSCF TH treatment is applied to more than one AVP in a message, the counter is only incremented once

Measurement Scope
Site

Recovery

1. No action required.

EvAfTopologyExceptionMp

Measurement ID
14040

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given exception treatment while applying S9 AF/pCSCF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 AF/pCSCF TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, or ATH and "AF/pCSCF Actual Name Not Found" Action is invoked

Measurement Scope
Site

Recovery

1. No action required.

EvAfTopologyException

Measurement ID
14041

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given exception treatment while applying S9 AF/pCSCF topology hiding treatment

Collection Interval
5 min

Peg Condition
When S9 AF/pCSCF TH treatment is applied to either a Request or Answer message at TH trigger points RTH, RTR, or ATH and "AF/pCSCF Actual Name Not Found" Action is invoked

Measurement Scope
Site

Recovery

1. No action required.

TxPathTopologyMp

Measurement ID
14024

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given path topology hiding treatment on messages routed to an Untrusted Network

Collection Interval
5 min

Peg Condition
Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTH and ATH respectively

Measurement Scope
Site

Recovery

1. No action required.

RxPathTopologyMp

Measurement ID
14025

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given path topology hiding treatment on messages routed from an Untrusted Network

Collection Interval
5 min

Peg Condition
Each time Path TH treatment is applied to either a Request or Answer message at TH trigger points RTH and ATH respectively

Measurement Scope
Site

Recovery

1. No action required.

EvHssTopologyMp

Measurement ID
14026

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by Connection ID)

Description
The number of messages given S6a/S6d HSS topology hiding treatment

Collection Interval
5 min

Peg Condition
Each time S6a/S6d HSS TH treatment is applied to either a Request or Answer message a TH trigger points RTH, RTR, ATH, and ATR

> **Note:** If S6a/S6d HSS TH treatment is applied to more than one AVP in a message, the counter is only incremented once

Measurement Scope
Site

Recovery

1. No action required.

EvMmeTopologyMp

Measurement ID
14027

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given MME/SGSN topology hiding treatment

Collection Interval
5 min

Peg Condition
Each time MME/SGSN TH treatment is applied to either a Request or Answer message a TH trigger points RTH, RTR, ATH, and ATR

> **Note:** If MME/SGSN TH treatment is applied to more than one AVP in a message, the counter is only incremented once

Measurement Scope
Site

Recovery

1. No action required.

EvMmeTopologyExceptionMp

Measurement ID
14028

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given exception treatment while applying MME/SGSN topology hiding treatment

Collection Interval
5 min

Peg Condition
Each time MME/SGSN TH treatment is applied to either a Request or Answer message a TH trigger points RTH and ATH trigger points

Measurement Scope
Site

Recovery

1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set

EvHssTopologyExceptionMp

Measurement ID
14030

Measurement Group
Topology Hiding Performance

Measurement Type
Simple

Measurement Dimension
Single

Description
The number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment

Collection Interval
5 min

Peg Condition
When S6a/S6d HSS TH excpetion treatment is applied to Request at RTH trigger point

Measurement Scope
Site

Recovery

1. Check with the HSS Vendor and request the vendor to be RFC 6733 Compliant.

ESPR Measurements

Table 5-3 ESPR Measurements

Measurement Tag	Description	Collection Interval
EvAeConvertToProvSubFailed	Total number of failed attempts to convert an auto-enrolled subscriber to a provisioned subscriber	5 minutes
EvAeProvCreateSubFailed	Total number of failed attempts to create an auto-enrolled subscriber via the provisioning interface	5 minutes
EvAeShCreateSubFailed	Total number of failed attempts to create an auto-enrolled subscriber via the Sh interface	5 minutes

Table 5-3 (Cont.) ESPR Measurements

Measurement Tag	Description	Collection Interval
EvAeShDeleteSubFailed	Total number of failed attempts to delete an auto-enrolled subscriber via the Sh interface	5 minutes
RxAeConvertToProvSubSuccess	Total number of auto-enrolled subscribers converted to provisioned subscribers	5 minutes
RxAeProvCreateMsgs	Total number of requests received via the provisioning interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber	5 minutes
RxAeProvCreateSubSuccess	Total number of auto-enrolled subscribers created via the provisioning interface	5 minutes
RxAeShCreateSubSuccess	Total number of auto-enrolled subscribers created via the Sh interface	5 minutes
RxAeShDeleteSubMsgs	Total number of unsubscribe requests received via the Sh interface that triggered the removal of an auto-enrolled subscriber	5 minutes
RxAeShDeleteSubSuccess	Total number of auto-enrolled subscribers deleted via the Sh Interface	5 minutes
RxAeShPurCreateMsgs	Total number of update requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber	5 minutes
RxAeShSnrCreateMsgs	Total number of subscribe requests received via the Sh interface where the subscriber was unknown and auto-enrollment was triggered to create the subscriber	5 minutes
RxAeSnrCreateSubSuccess	Total number of auto-enrolled subscribers successfully created via the Sh interface	5 minutes
RxUdrBePnNonPooledEntity	Total number of update requests that generated notification(s) for non-pooled entity(s)	5 minutes
RxUdrBePnPooledEntity	Total number of update requests that generated notifications(s) for pooled entity(s)	5 minutes
RxUdrBeReadMsgs	Total number of read requests received	5 minutes

Table 5-3 (Cont.) ESPR Measurements

Measurement Tag	Description	Collection Interval
RxUdrBeUpdateMsgs	Total number of update requests received	5 minutes
RxUdrNmNotifAck	Total number of notification delivery responses received	5 minutes
RxUdrNmNotifAckAsAvailable	Total number of notifications successfully sent to the AS (the AS received the notification)	5 minutes
RxUdrNmNotifAckAsUnavailable	Total number of notifications that failed to be sent to the AS (the AS did not receive the notification)	5 minutes
RxUdrNmNotifAckLateResponse	Total number of notification delivery responses received after the delivery timeout period expired	5 minutes
RxUdrNmNotifAckNotSubscribed	Total number of notification delivery responses received that indicated the AS was not subscribed to the subscriber	5 minutes
RxUdrNmNotifAckTimeout	Total number of notification delivery requests sent where a response was not received within the configured timeout interval	5 minutes
RxUdrSmSubscribeMsgs	Total number of subscribe requests received	5 minutes
RxUdrSmSubscribeSnoFull	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	5 minutes
RxUdrSmUnsubscribeMsgs	Total number of unsubscribe requests received	5 minutes
RxUdrSmUnsubscribeNsNotFound	Total number of unsubscribe requests where the subscriber exists but the desired **notification subscription** does not exist	5 minutes
SQRQuotaRowElementsReset	Total number of Quota Row Elements got reset or the value of the nextResetTime element has been updated. (Pools+Subscribers)	5 minutes
SQRRecordsExamined	Total number of Records scanned by the Quota Reset Tasks (Pools+Subscribers)	5 minutes

Table 5-3 (Cont.) ESPR Measurements

Measurement Tag	Description	Collection Interval
SQRRecordsFailed	Total number of Records on which Quota Resets or nextResetTime update has Failed (Pools+Subscribers)	5 minutes
SQRRecordsReset	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)	5 minutes
TxUdrBeReadReqFailed	Total number of failed read requests	5 minutes
TxUdrBeReadReqSuccess	Total number of successful read requests	5 minutes
TxUdrBeReadTooMuchData	Total number of read requests could not be processed because user data size exceeds maximum size	5 minutes
TxUdrBeReadUnkSubscriber	Total number of read requests received where the subscriber was unknown	5 minutes
TxUdrBeUpdateInvalidEntity	Total number of update requests received where an unknown entity was encountered	5 minutes
TxUdrBeUpdateNotPoolMember	Total number of update requests received where a pooled entity was being updated, but the subscriber was not a member of a pool	5 minutes
TxUdrBeUpdateOutOfSync	Total number of update requests received where the incorrect sequence number to perform was supplied	5 minutes
TxUdrBeUpdateReqFailed	Total number of failed update requests	5 minutes
TxUdrBeUpdateReqSuccess	Total number of successful update requests	5 minutes
TxUdrBeUpdateTooBusy	Total number of update requests which could not be processed because of congestion	5 minutes
TxUdrBeUpdateUnkSubscriber	Total number of update requests received where the subscriber was unknown	5 minutes
TxUdrNmNotifComAgentError	Total number of notification delivery requests sent that resulted in a ComAgent delivery failure of the notification delivery request	5 minutes
TxUdrNmNotifDeletedTableFull	Total number of notifications that were deleted because the maximum configured number of outstanding notifications allowed had been exceeded	5 minutes

Table 5-3 (Cont.) ESPR Measurements

Measurement Tag	Description	Collection Interval
TxUdrNmNotifExceededMaxDel	Total number of notifications that exceeded the maximum configured number of delivery attempts allowed	5 minutes
TxUdrNmNotifExceededMaxTtl	Total number of notifications that exceeded the maximum configured time to live	5 minutes
TxUdrNmNotifNoValidEntity	Total number of notifications to be sent that did not consist of any valid entities	5 minutes
TxUdrNmNotifSent	Total number of notification delivery requests sent	5 minutes
TxUdrNmNotifTooMuchData	Total number of unsubscribe requests which could not be processed because UserData size exceeds maximum size	
TxUdrSmSubscribeReqFailed	Total number of failed subscribe requests	5 minutes
TxUdrSmSubscribeReqSuccess	Total number of successful subscribe requests	5 minutes
TxUdrSmSubscribeTooMuchData	Total number of subscribe requests which could not be processed because UserData size exceeds maximum size	
TxUdrSmSubscribeUnkSubscriber	Total number of subscribe requests received where the subscriber was unknown and was not added via auto-enrollment	5 minutes
TxUdrSmUnsubscribeReqFailed	Total number of failed unsubscribe requests	5 minutes
TxUdrSmUnsubscribeReqSuccess	Total number of successful unsubscribe requests	5 minutes
TxUdrSmUnsubscribeTooMuchData	Total number of notifications to be sent for which user data size exceeds maximum size	5 minutes
TxUdrSmUnsubscribeUnkSubscriber	Total number of unsubscribe requests received where the subscriber was unknown	5 minutes

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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

RxAeShCreateSubSuccess

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:

1. No action required.

RxAeShDeleteSubMsgs

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:

1. No action required.

RxAeShDeleteSubSuccess

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:

1. No action required.

RxAeShPurCreateMsgs

Measurement Group:
Auto Enrollment

Measurement Type:
Simple

Description:
Total number of update 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 an update request, the subscriber user identity is not found in the index, the subscribe request matches auto-enrollment requirements, and auto-enrollment for PUR is enabled.

Measurement Scope:
All

Recovery:

1. No action required.

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:

1. No action required.

RxAeSnrCreateSubSuccess

Measurement Group:
Auto Enrollment

Measurement Type:
Simple

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

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a subscriber is successfully created via the Sh interface.

Measurement Scope:
All

Recovery:

1. No action required.

RxUdrBePnNonPooledEntity

Measurement Group:
UDRBE Performance

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:

1. 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:

Recovery:

1. 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:

1. No action required.

RxUdrBeUpdateMsgs

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of update requests received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the UDR Back End receives an 'update' stack event.

Measurement Scope:
All

Recovery:

1. No action required.

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.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

RxUdrSmUnSubscribeMsgs

Measurement Group:
Subscription Management

Measurement Type:
Simple

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:

1. 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:

1. 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 a PUR Reset message arrives at Sh Interface.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

TxUdrBeReadTooMuchData

Measurement Group:
UDRBE Exceptions

Measurement Type:
Simple

Description:
Total number of read requests could not be processed because user data size exceeds maximum size.

Collection Interval:
5 min

Peg Condition:
The measurement shall be incremented each time the UDR back end received a read request with user data which exceeds maximum size.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

TxUdrNmNotifTooMuchData

Measurement Group:
UDRBE Exceptions

Measurement Type:
Simple

Description:
Total number of notifications to be sent for which user data size exceeds maximum size.

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the UDR back end has user data to be sent in notify event and the size of user data exceeds maximum size.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. No action required.

TxUdrSmSubscribeTooMuchData

Measurement Group:
UDRBE Exceptions

Measurement Type:
Simple

Description:
Total number of subscribe requests which could not be processed because user data size exceeds maximum size.

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the UDR back end has user data to be sent in subscribe response and the size of user data exceeds maximum size.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. No action required.

TxUdrSmUnsubscribeTooMuchData

Measurement Group:
UDRBE Exceptions

Measurement Type:
Simple

Description:
Total number of unsubscribe requests which could not be processed because user data size exceeds maximum size.

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the UDR back end has user data to be sent in unsubscribe response and the size of user data exceeds maximum size.

Measurement Scope:
All

Recovery:

1. No action required.

TxUdrSmUnSubscribeUnkSubscriber

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:

1. No action required.

Pool Spanning Measurements

Table 5-4 Pool Spanning Measurements

Measurement Tag	Description	Collection Interval
PSO Inter-NO Traffic measurements (Remote Pool Member Host Read Request)		
TxUdrBePsoReadMsgs	Total number of PSO read requests sent due to a read request.	5 min
RxUdrBePsoReadSuccess	Total number of PSO read responses received indicating success.	5 min
RxUdrBePsoReadUnkPool	Total number of PSO read responses received where the pool did not exist.	5 min
RxUdrBePsoReadFailed	Total number of PSO read responses received that failed.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Member Host Subscribe with Read Request)		
TxUdrSmPsoReadMsgs	Total number of PSO read requests sent due to a subscribe request.	5 min
RxUdrSmPsoReadSuccess	Total number of PSO read responses received due to a subscribe request indicating success.	5 min
RxUdrSmPsoReadUnkPool	Total number of PSO read responses received due to a subscribe request where the pool did not exist.	5 min
RxUdrSmPsoReadFailed	Total number of PSO read responses received due to a subscribe request that failed.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Host Read Request)		
RxUdrBePsoReadMsgs	Total number of PSO read requests received.	5 min
TxUdrBePsoReadSuccess	Total number of PSO read requests processed.	5 min

Table 5-4 (Cont.) Pool Spanning Measurements

Measurement Tag	Description	Collection Interval
TxUdrBePsoReadUnkPool	Total number of PSO read requests that could not be processed because the pool did not exist.	5 min
TxUdrBePsoReadFailed	Total number of PSO read responses processed that failed.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Member Host Update Request)		
TxUdrBePsoUpdateMsgs	Total number of PSO update requests sent.	5 min
RxUdrBePsoUpdateSuccess	Total number of PSO update responses received.	5 min
RxUdrBePsoUpdateUnkPool	Total number of PSO update responses received where the pool did not exist.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Member Host Update Request)		
RxUdrBePsoUpdateOutOfSync	Total number of PSO update responses received where the incorrect sequence number was supplied.	5 min
RxUdrBePsoUpdateInvalidEntity	Total number of PSO update responses received where an unknown entity was encountered.	5 min
RxUdrBePsoUpdateTooBusy	Total number of PSO update responses received where the request could not be processed because of congestion.	5 min
RxUdrBePsoUpdateFailed	Total number of PSO update responses received that failed.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Host Update Request)		
RxUdrBePsoUpdateMsgs	Total number of PSO update requests received.	5 min
TxUdrBePsoUpdateSuccess	Total number of PSO update responses sent.	5 min
TxUdrBePsoUpdateUnkPool	Total number of PSO update messages that could not be processed because the pool did not exist.	5 min
TxUdrBePsoUpdateOutOfSync	Total number of PSO update messages where the incorrect sequence number was supplied.	5 min
TxUdrBePsoUpdateInvalidEntity	Total number of PSO update messages where an unknown entity was encountered.	5 min

Table 5-4 (Cont.) Pool Spanning Measurements

Measurement Tag	Description	Collection Interval
TxUdrBePsoUpdateTooBusy	Total number of PSO update messages where the request could not be processed because of congestion.	5 min
TxUdrBePsoUpdateFailed	Total number of PSO update messages processed that failed.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Host Notify Processing)		
TxUdrBePsoNotifyMsgs	Total number of PSO notify messages sent.	5 min
RxUdrBePsoNotifySuccess	Total number of PSO notify response messages received.	5 min
RxUdrBePsoNotifyNoMembers	Total number of PSO notify response messages received where no local members were found in the pool.	5 min
RxUdrBePsoNotifyPoolNotExist	Total number of PSO notify response messages received where the pool did not exist.	5 min
PSO Inter-NO Traffic measurements (Remote Pool Member Host Notify Processing)		
RxUdrBePsoNotifyMsgs	Total number of PSO notify messages received.	5 min
TxUdrBePsoNotifySuccess	Total number of PSO notify response messages sent.	5 min
TxUdrBePsoNotifyNoMembers	Total number of PSO notify response messages sent where no local members were found in the pool.	5 min
TxUdrBePsoNotifyPoolNotExist	Total number of PSO notify response messages sent where the pool did not exist.	5 min
PSO Inter-NO Traffic measurements (Get PSO Pool Membership Processing)		
RxUdrBePsoGetMembersMsgs	Total number of PSO get members requests received.	5 min
RxUdrBePsoGetMembersSuccess	Total number of PSO get members responses received indicating success.	5 min
RxUdrBePsoGetMembersFailed	Total number of PSO get members responses received that failed.	5 min
RxUdrBePsoGetMembersUnkPool	Total number of PSO get members responses received where the pool did not exist.	5 min

Table 5-4 (Cont.) Pool Spanning Measurements

Measurement Tag	Description	Collection Interval
TxUdrBePsoGetMembersMsgs	Total number of PSO get members messages sent due to a provisioning GetAllPoolMembers request.	5 min
TxUdrBePsoGetMembersSuccess	Total number of PSO get members responses processed.	5 min
TxUdrBePsoGetMembersUnkPool	Total number of PSO get members requests that could not be processed because the pool did not exist.	5 min
PSO Inter-NO Traffic measurements (Exception Measurements)		
RxUdrBePsoReadTimeOut	Total number of PSO read requests that timed out.	5 min
RxUdrSmPsoReadTimeOut	Total number of PSO read requests due to a subscribe request that timed out.	5 min
RxUdrBePsoUpdateTimeOut	Total number of PSO update requests that timed out.	5 min
RxUdrBePsoNotifyTimeOut	Total number of PSO notify messages that timed out.	5 min
RxUdrBePsoGetMembersTimeOut	Total number of PSO get members requests sent for which a timely response was not received.	5 min
Failures of update, read and subscribe requests due to the PSO request failing		
TxUdrBeUpdateReqPsoFailed	Total number of update requests where the PSO update request failed.	5 min
TxUdrBeReadReqPsoFailed	Total number of read requests where the PSO read request failed.	5 min
TxUdrSmSubscribeReqPsoFailed	Total number of subscribe requests where the PSO read request failed.	5 min
TxUdrBePsoGetMembersFailed	Total number of PSO get members responses processed that failed.	5 min
PSO Summary Measurements (for KPIs)		
TxUdrBePsoRequest	Total number of PSO events sent.	5 min
RxUdrBePsoRequest	Total number of PSO events received.	5 min
PSO Request Latency		
UdrBePsoTransTimeMax	Maximum PSO transaction life-time in milliseconds.	5 min
UdrBePsoTransTimeAvg	Average PSO transaction life-time in milliseconds.	5 min

RxUdrBePsoGetMembersFailed

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get members responses received that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a get members response fails.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoGetMembersMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get member requests received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO get members request is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoGetMembersSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get members responses received indicating success

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO get members response received is successful.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoGetMembersTimeOut

Measurement Group:
UDRBE Exception

Measurement Type:
Simple

Description:
Total number of PSO get members requests sent for which a timely response was not received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a get members request times out.

Measurement Scope:
Server Group

Recovery:

1. Investigate the reason for the request timing out. The ComAgent links may be down due to network problems. If not, the network latency may be preventing the responses from being delivered before timing out.

RxUdrBePsoGetMembersUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get members responses received where the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the PSO read response is received where the pool did not exist.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoNotifyMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify messages received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO notify message is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoNotifyNoMembers

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify response messages received where no local members were found in the pool

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO notify response is received and no local members are found in the pool.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoNotifyPoolNotExist

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify response messages received where the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO notify response message is received and the related pool does not exist.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoNotifySuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify response messages sent

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO notify response message is sent.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoNotifyTimeout

Measurement Group:
UDRBE Exception

Measurement Type:
Simple

Description:
Total number of PSO notify messages that timed out

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO notify message times out

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoReadFailed

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses received that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the PSO reads a message.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoReadMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read requests received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read request is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoReadSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses received indicating success

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a successful PSO read response is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoReadTimeOut

Measurement Group:
UDRBE Exception

Measurement Type:
Simple

Description:
Total number of PSO read requests that timed out

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read request times out.

Measurement Scope:
Server Group

Recovery:

1. Investigate the reason for the request timing out. The ComAgent links may be down due to network problems. If not, the network latency may be preventing the responses from being delivered before timing out.

RxUdrBePsoReadUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses received where the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the PSO read response is received where the pool did not exist.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoRequest

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of PSO events received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the UDRBE receives a request from another user data repository in the pool network.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateFailed

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update responses received that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the PSO reads a message.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateInvalidEntity

Measurement Group:
PSO Performance

Measurement Type:
Simple

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

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update response is received that contains an unknown entity.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update requests received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update request is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateOutOfSync

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update responses received where the incorrect sequence number was supplied

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update response is received that contains an incorrect sequence number.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update responses received

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update response is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateTimeOut

Measurement Group:
UDRBE Exception

Measurement Type:
Simple

Description:
Total number of PSO update requests that timed out

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update request times out.

Measurement Scope:
Server Group

Recovery:

1. Investigate the reason for the request timing out. The ComAgent links may be down due to network problems. If not, the network latency may be preventing the responses from being delivered before timing out.

RxUdrBePsoUpdateTooBusy

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update responses received where the request could not be processed because of congestion

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update response is received and cannot be processed because of congestion.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBePsoUpdateUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update responses received where the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update response containing a nonexistent pool is encountered.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrSmPsoReadFailed

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses received due to a subscribe request that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read response is received due to a subscribe request that fails.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrSmPsoReadSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses received due to a subscribe request indicating success

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a successful PSO read response is received for subscriber request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrSmPsoReadTimeOut

Measurement Group:
UDRBE Exception

Measurement Type:
Simple

Description:
Total number of PSO read requests due to a subscribe request that timed out

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read request due to a subscribe request times out.

Measurement Scope:
Server Group

Recovery:

1. Investigate the reason for the request timing out. The ComAgent links may be down due to network problems. If not, the network latency may be preventing the responses from being delivered before timing out.

RxUdrSmPsoReadUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses received due to a subscribe request where the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read response is received due to a subscribe request containing a nonexistent pool.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoGetMembersFailed

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of PSO get members responses processed that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO get-members response fails to be processed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoGetMembersMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get members messages sent due to a provisioning GetAllPoolMembers request

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO get members message is sent due to a GetAllPoolMembers request. This request is sent to obtain the pool membership data stored on any other system in the PSO network.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoGetMembersSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get members responses processed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO get members request is processed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoGetMembersUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO get members requests that could not be processed because the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a members request cannot be processed because the pool does not exist.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoNotifyMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify messages sent

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO notify message is sent.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoNotifyNoMembers

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify response messages sent where no local members were found in the pool

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time no members are found for the pool and the UDR stores, updates, or deletes the pool register locally, returning an error response to the remote pool host indicating that no members exist in the pool.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoNotifyPoolNotExist

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify response messages sent where the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time an error response occurs when a PSO notify response message is sent and the related pool does not exist on the local host.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoNotifySuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO notify response messages sent

Collection Interval:
5 min

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

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoReadFailed

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read responses processed that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read response fails to be processed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoReadMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read requests sent due to a read request

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read request is sent because of a read request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoReadSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read requests processed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the PSO successfully processes a message.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoReadUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read requests that could not be processed because the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read request could not be processed because it contains a nonexistent pool.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoRequest

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of PSO events sent

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a request is sent to another system in the pool network.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateFailed

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update messages processed that failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update message fails.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateInvalidEntity

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update messages where an unknown entity was encountered

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update message with an unknown entity is encountered.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update requests sent

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update request is sent.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateOutOfSync

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update messages where the incorrect sequence number was supplied

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update message is encountered with an incorrect sequence number.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateSuccess

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update responses sent

Collection Interval:
5 min

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

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateTooBusy

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update messages where the request could not be processed because of congestion

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update message could not be processed due to congestion.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBePsoUpdateUnkPool

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO update messages that could not be processed because the pool did not exist

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO update message cannot be processed because the referenced pool does not exist.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBeReadReqPsoFailed

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of read requests where the PSO read request failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a read request sent to a remote pool does not complete successfully.

Measurement Scope:
Server Group

Recovery:

1. The read request from the MP failed because the read request sent to a remote pool host did not complete successfully. Investigate the cause of the failure on the remote pool host.

TxUdrBeUpdateReqPsoFailed

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of update requests where the PSO update request failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time an update request is sent to a remote pool host and does not complete successfully.

Measurement Scope:
Server Group

Recovery:

1. The update request from the MP failed because the update request sent to a remote pool host did not complete successfully. Investigate the cause of the failure on the remote pool host.

TxUdrSmPsoReadMsgs

Measurement Group:
PSO Performance

Measurement Type:
Simple

Description:
Total number of PSO read requests sent due to a subscribe request

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO read request is sent due to a subscribe request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrSmSubscribeReqPsoFailed

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Total number of subscribe requests where the PSO read request failed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the PSO reads a message.

Measurement Scope:
Server Group

Recovery:

1. The subscribe (with read) request from the MP failed because the read request sent to a remote pool host did not complete successfully. Investigate the cause of the failure on the remote pool host.

UdrBePsoTransTimeAvg

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Average PSO transaction life-time in milliseconds

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO transaction ends.

Measurement Scope:
Server Group

Recovery:

1. No action required.

UdrBePsoTransTimeMax

Measurement Group:
UDRBE Performance

Measurement Type:
Simple

Description:
Maximum PSO transaction life-time in milliseconds

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time a PSO transaction ends.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TTG Performance measurements

The TTG Performance measurement report contains measurements that provide performance information that is specific to each local TTG.

TtgMaxLossExceeded

Measurement ID
14349

Measurement Group
TTG Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTG ID)

Description
The number of request messages that were not routed to the TTG because the maximum loss rate for the Route Group in the Route List was exceeded.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Route Group is selected from a Route List and these criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG is owned by the local DSR Node
- Request message's Application-Id matches the Application-Id assigned to the local TTG
- TTG's Admin State = Enabled
- TTG's Current Loss Percent is greater than the TTG Max Loss Percent Threshold attribute value assigned to the Route Group within the Route List

Measurement Scope
Site

Recovery

1. No action required.

TtgSelectedP0

Measurement ID
14344

Measurement Group
TTG Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTG ID)

Description
The number of messages routed to the TTG with message priority 0.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Route Group is selected from a Route List and these criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG is owned by the local DSR Node
- Request message's Application-Id matches the Application-Id assigned to the local TTG
- TTG's Admin State = Enabled
- TTG's Current Loss Percent is less than or equal to the TTG Max Loss Percent Threshold attribute value assigned to the Route Group within the Route List
- Message Priority = 0

Measurement Scope
Site

Recovery

1. No action required.

TtgSelectedP1

Measurement ID
14345

Measurement Group
TTG Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTG ID)

Description
The number of messages routed to the TTG with message priority 1.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Route Group is selected from a Route List and these criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG is owned by the local DSR Node

- Request message's Application-Id matches the Application-Id assigned to the local TTG
- TTG's Admin State = Enabled
- TTG's Current Loss Percent is less than or equal to the TTG Max Loss Percent Threshold attribute value assigned to the Route Group within the Route List
- Message Priority = 1

Measurement Scope
Site

Recovery

1. No action required.

TtgSelectedP2

Measurement ID
14346

Measurement Group
TTG Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTG ID)

Description
The number of messages routed to the TTG with message priority 2.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Route Group is selected from a Route List and these criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG is owned by the local DSR Node
- Request message's Application-Id matches the Application-Id assigned to the local TTG
- TTG's Admin State = Enabled
- TTG's Current Loss Percent is less than or equal to the TTG Max Loss Percent Threshold attribute value assigned to the Route Group within the Route List
- Message Priority = 2

Measurement Scope
Site

Recovery

1. No action required.

TtgSelectedPrimaryTtg

Measurement ID
14347

Measurement Group
TTG Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTG ID)

Description
The number of request messages routed to the TTG where the TTG is associated with the primary Route Group in the Route List.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Route Group is selected from a Route List and these criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG is owned by the local DSR Node
- Request message's Application-Id matches the Application-Id assigned to the local TTG
- TTG's Admin State = Enabled
- TTG's Current Loss Percent is less than or equal to the TTG Max Loss Percent Threshold attribute value assigned to the Route Group within the Route List
- Route Group within Route List is the current Active Route Group for the Route List

Measurement Scope
Site

Recovery

1. No action required.

TtgSelectedSecondaryTtg

Measurement ID
14348

Measurement Group
TTG Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTG ID)

Description
The number of request messages routed to the TTG where the TTG is associated with a secondary Route Group in the Route List.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Route Group is selected from a Route List and these criteria are met:

- TTG is assigned to the Route Group within the Route List
- TTG is owned by the local DSR Node
- Request message's Application-Id matches the Application-Id assigned to the local TTG
- TTG's Admin State = Enabled
- TTG's Current Loss Percent is less than or equal to the TTG Max Loss Percent Threshold attribute value assigned to the Route Group within the Route List
- Route Group within Route List is not the current Active Route Group for the Route List

Measurement Scope
Site

Recovery

1. No action required.

TtgTmLossRateRange1

Measurement ID
14340

Measurement Group
TTG Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTG ID)

Description
Duration of TTG Loss Percent Range1

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"
- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of the time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values
  - Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtgTmLossRateRange2

Measurement ID
14341

Measurement Group
TTG Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTG ID)

Description
Duration of TTG Loss Percent Range2

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"

- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of the time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values
  - Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtgTmLossRateRange3

Measurement ID
14342

Measurement Group
TTG Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTG ID)

Description
Duration of TTG Loss Percent Range3

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"
- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of the time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values

- Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtgTmLossRateRange4

Measurement ID
14343

Measurement Group
TTG Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTG ID)

Description
Duration of TTG Loss Percent Range4

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"
- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of the time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values
  - Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TTP Performance measurements

The TTP Performance measurement report contains measurements that provide performance information that is specific to each TTP.

TtpDivertedInP0G

Measurement ID
14328

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were diverted from another TTP, with message priority 0 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction is marked as "TTP Diverted" in its PTR
- Message Priority = 0
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedInP0Y

Measurement ID
14331

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were diverted from another TTP, with message priority 0 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction is marked as "TTP Diverted" in its PTR
- Message Priority = 0
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedInP1G

Measurement ID
14329

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were diverted from another TTP, with message priority 1 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction is marked as "TTP Diverted" in its PTR
- Message Priority = 1

- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedInP1Y

Measurement ID
14332

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were diverted from another TTP, with message priority 1 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction is marked as "TTP Diverted" in its PTR
- Message Priority = 1
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedInP2G

Measurement ID
14330

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were diverted from another TTP, with message priority 2 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction is marked as "TTP Diverted" in its PTR
- Message Priority = 2
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedInP2Y

Measurement ID
14333

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were diverted from another TTP, with message priority 2 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction is marked as "TTP Diverted" in its PTR

- Message Priority = 2
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedOutP0G

Measurement ID
14316

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were throttled/diverted, with message priority 0 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was diverted
- Message Priority = 0
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedOutP0Y

Measurement ID
14319

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were throttled/diverted, with message priority 0 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was diverted
- Message Priority = 0
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedOutP1G

Measurement ID
14317

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were throttled/diverted, with message priority 1 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was diverted

- Message Priority = 1
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedOutP1Y

Measurement ID
14320

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were throttled/diverted, with message priority 1 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was diverted
- Message Priority = 1
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedOutP2G

Measurement ID
14318

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were throttled/diverted, with message priority 2 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was diverted
- Message Priority = 2
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDivertedOutP2Y

Measurement ID
14321

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were throttled/diverted, with message priority 2 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was diverted

- Message Priority = 2
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDoicException

Measurement ID
14300

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of DOIC Protocol Errors.

Collection Interval
5 min

Peg Condition
This measurement is incremented whenever event TtpEvDoicException is generated.

Measurement Scope
Site

Recovery

1. No action required.

TtpDropP0G

Measurement ID
14322

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of transactions abandoned due to TTP throttling/diversion, with message priority 0 and color green.

Collection Interval
5 min

Peg Condition
The DRL abandoned routing of a transaction and all of these criteria are met:

- Last routing failure encountered was due to TTP diversion
- Message Priority = 0
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDropP0Y

Measurement ID
14325

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of transactions abandoned due to TTP throttling/diversion, with message priority 0 and color yellow.

Collection Interval
5 min

Peg Condition
The DRL abandoned routing of a transaction and all of these criteria are met:

- Last routing failure encountered was due to TTP diversion
- Message Priority = 0
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDropP1G

Measurement ID
14323

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of transactions abandoned due to TTP throttling/diversion, with message priority 1 and color green.

Collection Interval
5 min

Peg Condition
The DRL abandoned routing of a transaction and all of these criteria are met:

- Last routing failure encountered was due to TTP diversion
- Message Priority = 1
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDropP1Y

Measurement ID
14326

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of transactions abandoned due to TTP throttling/diversion, with message priority 1 and color yellow.

Collection Interval
5 min

Peg Condition
The DRL abandoned routing of a transaction and all of these criteria are met:

- Last routing failure encountered was due to TTP diversion
- Message Priority = 1
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpDropP2G

Measurement ID
14324

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of transactions abandoned due to TTP throttling/diversion, with message priority 2 and color green.

Collection Interval
5 min

Peg Condition
The DRL abandoned routing of a transaction and all of these criteria are met:

- Last routing failure encountered was due to TTP diversion
- Message Priority = 2
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpDropP2Y

Measurement ID
14327

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of transactions abandoned due to TTP throttling/diversion, with message priority 2 and color yellow.

Collection Interval
5 min

Peg Condition
The DRL abandoned routing of a transaction and all of these criteria are met:

- Last routing failure encountered was due to TTP diversion
- Message Priority = 2
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledDoicOverrideFlag

Measurement ID
14309

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not diverted due to priority override.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and the transaction was not diverted because the Request message priority is greater than or equal to the TTP's Override Message Priority Threshold attribute value.

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP0G

Measurement ID
14310

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 0 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 0
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP0Y

Measurement ID
14313

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 0 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 0
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP1G

Measurement ID
14314

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 1 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 1
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP1Y

Measurement ID
14314

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 1 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 1
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP2G

Measurement ID
14312

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 2 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 2
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP2Y

Measurement ID
14315

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 2 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 2
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP4G

Measurement ID
14335

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 4 and color green.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 4
- Message Color = Green

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledP4Y

Measurement ID
14336

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP which were not throttled, with message priority 4 and color yellow.

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and all of these criteria are met:

- Transaction was not diverted
- Message Priority = 4
- Message Color = Yellow

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledRateAvg

Measurement ID
14307

Measurement Group
TTP Performance

Measurement Type
Average

Measurement Dimension
Arrayed (by TTP ID)

Description
Average TTP request message routing rate (messages per second).

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and the transaction was not diverted.

Measurement Scope
Site

Recovery

1. No action required.

TtpHandledRatePeak

Measurement ID
14306

Measurement Group
TTP Performance

Measurement Type
Max

Measurement Dimension
Arrayed (by TTP ID)

Description
Peak TTP request message routing rate (messages per second).

Collection Interval
5 min

Peg Condition
The TTP was selected as defined by the peg condition criteria defined for TtpSelected and the transaction was not diverted.

Measurement Scope
Site

Recovery

1. No action required.

TtpSelected

Measurement ID
14305

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of request messages routed to TTP.

Collection Interval
5 min

Peg Condition
This measurement is updated when a Peer Node or Connection is selected from a Route Group (or a Peer Node is selected or Destination-Host Implicit Routing) which has an active TTP associated with the transaction meeting the following criteria:

- Request message's Application-Id matches the Application-Id assigned to the TTP
- FQDN assigned to the selected Peer Node/Connection matches the FQDN of the Peer Node assigned to the TTP
- TTP's Throttling Admin State = Enabled

Measurement Scope
Site

Recovery

1. No action required.

TtpTmLossRateRange1

Measurement ID
14301

Measurement Group
TTP Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTP ID)

Description
The duration of TTP Loss Percent Range1.

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"

- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values
  - Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtpTmLossRateRange2

Measurement ID
14302

Measurement Group
TTP Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTP ID)

Description
The duration of TTP Loss Percent Range2.

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"
- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values

– Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtpTmLossRateRange3

Measurement ID
14303

Measurement Group
TTP Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTP ID)

Description
The duration of TTP Loss Percent Range3.

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"
- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  – Calculate the duration of time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  – Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values
  – Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtpTmLossRateRange4

Measurement ID
14304

Measurement Group
TTP Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTP ID)

Description
The duration of TTP Loss Percent Range4.

Collection Interval
5 min

Peg Condition
When the DRL changes a local TTG's Current Loss Percent value, it shall:

- Save the time of the event in the TTG's RT-DB record called "Loss Start Time"
- Save the new Current Loss Percent value in the TTG's RT-DB record
- If the TTG's old Current Loss Percent value is not equal to 0, then:
  - Calculate the duration of time that the TTG's Current Loss Percent was set to the previous value based upon "Loss Start Time" and the current time
  - Determine which TtgTmLossRateRange-X measurement to update based upon the previous TTG Current Loss Percent value and the system-wide LossRateMax1, LossRateMax2, and LossRateMax3 values
  - Update the selected TtgTmLossRateRange-X measurement with the calculated duration of time

Measurement Scope
Site

Recovery

1. No action required.

TtpTmStaticThrottling

Measurement ID
14334

Measurement Group
TTP Performance

Measurement Type
Duration

Measurement Dimension
Arrayed (by TTP ID)

Description
The duration of time (in seconds) that TTP Static Throttling was being applied.

Collection Interval
5 min

Peg Condition
The time duration interval starts when any of these events occur:

- The TTP's Operational Reason is changed to "Static Rate Limit Exceeded"
- A new measurement collection interval begins and the TTP's Operational Reason is "Static Rate Limit Exceeded"

The time duration interval stops when any of these events occur:

- The TTP's Operational Reason is changed from "Static Rate Limit Exceeded" to any other value
- The current measurement collection interval ends

When a time duration interval completes, the time measured is added to the total measurement value.

Measurement Scope
Site

Recovery

1. No action required.

TtpUniqueOLRs

Measurement ID
14308

Measurement Group
TTP Performance

Measurement Type
Simple

Measurement Dimension
Arrayed (by TTP ID)

Description
The number of unique **DOIC OLR**s successfully processed.

Collection Interval
5 min

Peg Condition
This measurement is updated when a DOIC OLR is accepted, applied to the associated TTP and the OLR's Sequence Number is greater than the TTP's Sequence Number.

Measurement Scope
Site

Recovery

1. No action required.

UDRFE Measurements

Table 5-5 **UDRFE *Measurements***

Measurement Tag	Description	Collection Interval
RxInvalidDataRefValue	Total number of SNR requests that contained an invalid DataReference AVP value	5 minutes
RxInvalidDelete	Total number of PUR requests that contained a delete request with a sequence number of 0	5 minutes
RxInvalidExpTimeValue	Total number of SNR requests that contained an invalid ExpiryTime AVP value	5 minutes
RxRequestAll	Total number of requests received	5 minutes
RxRequestDiscarded	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	5 minutes
RxRequestFailedAll	Total number of requests that failed to be processed due to errors	5 minutes
RxRequestFailedPUR	Total number of PUR requests that failed to be processed due to errors	5 minutes
RxRequestFailedSNR	Total number of SNR requests that failed to be processed due to errors	5 minutes
RxRequestFailedUDR	Total number of UDR requests that failed to be processed due to errors	5 minutes
RxRequestPUR	Total number of PUR requests received	5 minutes
RxRequestRejectedComAgentError	Total Number of Requests which cannot be processed due to ComAgent errors	5 minutes

Table 5-5 (Cont.) UDRFE Measurements

Measurement Tag	Description	Collection Interval
RxRequestRejectedInvalidServiceId	Total number of requests that cannot be processed due to invalid service indication	5 minutes
RxRequestRejectedMessageDecodingFailed	Total number of requests that cannot be processed due to message decoding failure	5 minutes
RxRequestRejectedPermissionsNotPresent	Total number of requests that cannot be processed because the host does not have the permissions to execute the operation.	5 minutes
RxRequestRejectedUnknownApplicationId	Total number of requests that cannot be processed due to unknown application ID	5 minutes
RxRequestRejectedUnknownUser	Total number of requests that cannot be processed due to unknown user	5 minutes
RxRequestSNR	Total number of SNR requests received	5 minutes
RxRequestSuccessfulAll	Total number of requests successfully processed	5 minutes
RxRequestSuccessfulPUR	Total number of PUR successfully processed	5 minutes
RxRequestSuccessfulSNR	Total number of SNR successfully processed	5 minutes
RxRequestSuccessfulUDR	Total number of UDR requests successfully processed	5 minutes
RxRequestUDR	Total number of UDR received	5 minutes
RxResetRequestPUR	Total number of PUR Quota Reset Request Messages Received	5 minutes
RxResetRequestPURFailed	Total number of PUR Quota Reset Requests failed	5 minutes
RxResetRequestPURSuccessful	Total number of PUR Quota Reset Request Messages successfully processed	5 minutes
RxResponseAll	Total Number of Responses received	5 minutes
RxResponsePNA	Total number of PNA received	5 minutes
RxResponseRejectedComAgentError	Total number of responses that cannot be processed due to ComAgent connection errors	5 minutes

Table 5-5 (Cont.) UDRFE Measurements

Measurement Tag	Description	Collection Interval
RxResponseRejectedMessageDecodingFailed	Total number of responses which cannot be processed due to message decoding failure	5 minutes
RxResponseRejectedUnknownApplicationId	Total number of responses which cannot be processed due to unknown application ID	5 minutes
RxTooMuchData	Total number of PUR requests that contained too much data to process	5 minutes
TmRemotePeerOrphanResponse	Response is received from Remote Diameter Peer for which no pending request event is found	5 minutes
TmPNAReceiveTimeOut	PNR is sent but transaction is timed out as PNA is not received in configured time	5 minutes
TmRemotePeerOrphanResponse	Response is received from Remote Diameter Peer for which no pending request event is found	5 minutes
TmResponseEventTimeOut	Request event is sent to UDRBE but transaction is timed out as UDRBE response event is not received in configured time	5 minutes
TmResponseTimeSPR	Average time from request to response	5 minutes
TmUdrAnsAvgQ	Average UDR answer queue utilization	5 minutes
TmUdrAnsPeakQ	Maximum UDR answer queue size utilization	5 minutes
TmUdrAvgStkEventQ	Average UDR stack event queue utilization	5 minutes
TmUdrbeOrphanResponse	Response event is received from UDRBE for which no pending request event is found	5 minutes
TmUdrPeakStkEventQ	Maximum UDR stack event queue size utilization	5 minutes
TmUdrReqAvgQ	Average UDR request queue utilization	5 minutes
TmUdrReqPeakQ	Maximum UDR request queue utilization	

Table 5-5 (Cont.) **UDRFE** ***Measurements***

Measurement Tag	Description	Collection Interval
TxPnaAsUnavailable	Total number of PNA responses received that indicate an AS is unavailable	5 minutes
TxPnrCreateFailed	Total number of PNR requests that failed to build	5 minutes
TxRequestAll	Total Number of Requests sent	5 minutes
TxRequestFailedAll	Total number of Requests that have failed to be processed due to errors	5 minutes
TxRequestFailedPNR	Total number of PNR requests that failed to be processed due to errors	5 minutes
TxRequestPNR	Total number of PNR sent to PCRF	5 minutes
TxRequestSuccessfulAll	Total Number of Requests successfully processed	5 minutes
TxRequestSuccessfulPNR	Total number of PNR requests successfully processed	5 minutes
TxResponseAll	Total number of responses sent	5 minutes
TxResponsePUA	Total number of PUA sent to PCRF	5 minutes
TxResponseSNA	Total number of SNA sent to PCRF	5 minutes
TxResponseUDA	Total number of UDA sent to PCRF	5 minutes

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:

1. 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:

1. No action required.

RxInvalidExpTimeValue

Measurement Group:
Sh Exceptions

Measurement Type:
Simple

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

Collection Interval:
5 min

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

Measurement Scope:
All

Recovery:

1. No action required.

RxRequestAll

Measurement Group:
UDRBE 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:

1. 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.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

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:

1. 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:

1. 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:

1. 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.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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.

Measurement Scope:
All

Recovery:

1. No action required.

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.

Measurement Scope:
All

Recovery:

1. No action required.

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.

Measurement Scope:
All

Recovery:

1. No action required.

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.

Measurement Scope:
All

Recovery:

1. No action required.

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:

1. 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:

1. 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:

1. No action required.

RxResponseRejectedComAgentError

Measurement Group:
Sh Exceptions

Measurement Type:
Simple

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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

TxPnaAsUnavailable

Measurement Group:
Sh Exceptions

Measurement Type:
Simple

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:

1. 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:

1. 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:

1. 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.

Measurement Scope:
All

Recovery:

1. No action required.

TxRequestPNR

Measurement Group:
Sh 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 is sent.

Measurement Scope:
All

Recovery:

1. 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.

Measurement Scope:
All

Recovery:

1. 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.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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 you to determine which provisioning rules are most commonly used and the percentage of times that messages were successfully (or unsuccessfully) routed.

Table 5-6 UDR RAS and XSAS Provisioning Related Measurements

Measurement Tag	Description	Collection Interval
ProvTxnCommitted	Total number of transactions successfully committed to the database (memory and on disk) on the active server of the primary site	5 min
RxCmdLogExportExecuted	Total number of Command Log Export tasks executed	5 min
RxProvExportCmds	Total number of commands exported	5 min
RxProvExportRequested	Total number of exports requested	5 min
RxProvExportsFailed	Total number of XML export requests that failed due to errors	5 min
RxProvExportsSuccessful	Total number of successful XML export requests	5 min
RxProvImportCmdsFailed	Total number of commands that failed import	5 min
RxProvImportCmdsSuccessful	Total number of commands that imported successfully	5 min
RxProvImportFilesFailed	Total number of files that failed to be imported due to errors	5 min

Table 5-6 (Cont.) UDR RAS and XSAS Provisioning Related Measurements

Measurement Tag	Description	Collection Interval
RxProvImportFilesReceived	Total number of provisioning files received from an import operation	5 min
RxProvImportFilesSuccessful	Total number of files imported successfully	5 min
RxRasDeleteReqReceived	Total number of REST DELETE requests that have been received on the provisioning interface	5 min
RxRasGetReqReceived	Total number of REST GET requests that have been received on the provisioning interface	5 min
RxRasPostReqReceived	Total number of REST POST requests that have been received on the provisioning interface	5 min
RxRasProvConnectionIdleTimeouts	Total number of connections that timed out and terminated due to idleness	5 min
RxRasProvConnectsAccepted	Total number of client initiated connect attempts that were accepted	5 min
RxRasProvConnectsAttempted	Total number of client initiated connect attempts to establish a connection with the server	5 min
RxRasProvConnectsDenied	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	5 min
RxRasProvMsgsDiscarded	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	5 min
RxRasProvMsgsFailed	Total number of provisioning messages that failed to be processed due to errors	5 min
RxRasProvMsgsReceived	Total number of provisioning messages received	5 min
RxRasProvMsgsSent	Total number of provisioning messages sent	5 min

Table 5-6 (Cont.) UDR RAS and XSAS Provisioning Related Measurements

Measurement Tag	Description	Collection Interval
RxRasProvMsgsSuccessful	Total number of provisioning messages successfully processed	5 min
RxRasPutReqReceived	Total number of REST PUT requests that have been received on the provisioning interface	5 min
RxRasResetReqReceivedRate	Total number of REST reset requests that have been received on the provisioning interface	5 min
RxXsasDeleteReqReceived	Total number of SOAP delete requests that have been received on the provisioning interface	5 min
RxXsasInsertReqReceived	The total number of SOAP insert requests that have been received on the provisioning interface.	5 min
RxXsasOperationReqReceived	Total number of SOAP operation requests that have been received on the provisioning interface	5 min
RxXsasProvConnectionIdleTimeouts	Total number of connections that timed out and terminated due to idleness	5 min
RxXsasProvConnectsAccepted	Total number of client initiated connect attempts that were accepted	5 min
RxXsasProvConnectsAttempted	Total number of client initiated connect attempts to establish a connection with the server	5 min
RxXsasProvConnectsDenied	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	5 min
RxXsasProvConnectsFailed	Total number of client initiated connect attempts that failed due to errors during initialization	5 min
RxXsasProvMsgsDiscarded	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	5 min

Table 5-6 (Cont.) UDR RAS and XSAS Provisioning Related Measurements

Measurement Tag	Description	Collection Interval
RxXsasProvMsgsFailed	Total number of provisioning messages that failed to be processed due to errors	5 min
RxXsasProvMsgsReceived	Total number of provisioning messages received	5 min
RxXsasProvMsgsSent	Total number of provisioning messages sent	5 min
RxXsasProvMsgsSuccessful	Total number of provisioning messages that were successfully processed	5 min
RxXsasProvTxnRequestsDiscarded	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	5 min
RxXsasProvTxnTotal	Total number of SOAP Transactions that have been attempted	5 min
RxXsasResetReqReceived	Total number of SOAP reset requests that have been received on the provisioning interface	5 min
RxXsasSelectReqReceived	Total number of SOAP select requests that have been received on the provisioning interface	5 min
RxXsasUpdateReqReceived	Total number of SOAP update requests that have been received on the provisioning interface	5 min
TotalPoolCount	The total number of pools in a 30-minute period	30 min
TotalSubscriberCount	The total number of subscribers in a 30-minute period	30 min
TxProvImportResultFilesTransferred	Total number of result files transferred	5 min
TxProvTxnAborted	Total number of transactions that were successfully aborted after a configured number of retries	5 min
TxProvTxnDurabilityTimeouts	Total number of committed, non-durable transactions that failed to become durable within the amount of time specified by Transaction Durability Timeout	5 min

Table 5-6 (Cont.) UDR RAS and XSAS Provisioning Related Measurements

Measurement Tag	Description	Collection Interval
TxProvTxnFailed	Total number of transactions that failed to be started or committed or were aborted due to errors	5 min
TxProvTxnTotal	Total number of transactions that were attempted (the sum of R_ProvTxnCommitted, R_ProvTxnTimeouts, R_ProvTxnAborted, and R_ProvTxnFailed counters)	5 min
TxXsasProvTxnAborted	Total number ofSOAPtransactions that have been aborted after configured number of retries	5 min
TxXsasProvTxnFailed	Total number of SOAP transactions that have failed to be started or committed	5 min
XsasProvTxnCommitted	Total number of Soap transactions that have been successfully committed to the database	5 min

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:

1. No action required.

RxCmdLogExportExecuted

Measurement Group:
Provisioning Performance

Measurement Type:
Simple

Description:
Total number of Command Log Export tasks executed

Collection Interval:
5 min

Peg Condition:
This measurement is incremented every time the Command Log export is initiated.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. No action required.

RxProvExportsFailed

Measurement Group:
Provisioning Exceptions

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:

1. 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:

1. 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:

1. 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.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

RxRasProvMsgsSuccessful

Measurement Group:
Provisioning Performance

Measurement Type:
Simple

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:

1. 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:

1. No action required.

RxRasResetReqReceived

Measurement Group:
Provisioning Performance

Measurement Type:
Simple

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

Collection Interval:
5 min

Peg Condition:
This measurement shall be incremented each time the Provisioning Front End receives a Reset request on the SOAP provisioning interface.

Measurement Scope:
All

Recovery:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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.

Measurement Scope:
All

Recovery:

1. No action required.

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.

Measurement Scope:
All

Recovery:

1. 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.

Measurement Scope:
All

Recovery:

1. 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.

Measurement Scope:
All

Recovery:

1. 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:

1. No action required.

RxXsasResetReqReceived

Measurement Group:
Provisioning Performance

Measurement Type:
Simple

Description:
Total number of SOAP reset 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 RESET request on the REST provisioning interface.

Measurement Scope:
All

Recovery:

1. 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:

1. 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 every time the Command Log export is initiated.

Measurement Scope:
All

Recovery:

1. No action required.

TotalPoolCount

Measurement Group:
Provisioning Performance

Measurement Type:
Max

Description:
Total number of pools reported in a 30-minute period

Collection Interval:
30 min

Peg Condition:
The calculation for this measurement is performed on a 30-minute interval. Once in a 30-minute period, the number of pools is queried from the database and reported. Note that for the first 30 minutes after an installation this measurement displays 0.

Measurement Scope:
All

Recovery:

1. No action required.

TotalSubscriberCount

Measurement Group:
Provisioning Performance

Measurement Type:
Max

Description:
Total number of subscribers reported in a 30-minute period

Collection Interval:
30 min

Peg Condition:
The calculation for this measurement is performed on a 30-minute interval. Once in a 30-minute period, the number of subscribers is queried from the database and reported. Note that for the first 30 minutes after an installation this measurement displays 0.

Measurement Scope:
All

Recovery:

1. No action required.

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:

1. 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:

1. 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:

1. 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:

1. 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:

1. 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:

1. No action required.

TxXsasProvTxnFailed

Measurement Group:
Provisioning Exceptions

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:

1. 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:

1. No action required.

Ud Client Measurements

The measurements in the Ud Client Measurements table appear in one of the four Ud client measurement reports available from the **Main Menu** > **Measurements** > **Report** GUI option:

- Ud Client Exception
- Ud Client LDAP Interface
- Ud Client Performance
- Ud Client SOAP Interface

Table 5-7 Ud Client Measurements

Measurement Tag	Description	Collection Interval
Ud Client Exceptions		
EvUdBindRequestTimedOut	Total number of LDAP Bind requests which timed out before a response was received.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
EvUdLDAPIdleConnectionDropped	Total number of times an LDAP connection has been disconnected after requests have been sent, but no data has been received within the configured time period.	5 min
EvUdLDAPTCPSendBufferFull	Total number of times an attempt to send an LDAP Search request on a connection has failed because the TCP/IP send buffer is full.	5 min
EvUdNotifyDeleteSubscriberFailed	Total number of subscribers indicated as deleted in a SOAP Notify request where the subscriber failed to be deleted.	5 min
EvUdNotifyFieldUpdateFailure	Total number of individual notifications within a SOAP Notify request which attempted to update a field to an invalid value according to the field definition in the SEC.	5 min
EvUdNotifyRequestTimeout	Total number of SOAP Notify requests that were sent by the Ud Client application to the UDR BE for which no response was received within the expected time period.	5 min
EvUdNotifyUnexpectedUpdateField	Total number of individual notifications within a SOAP Notify request which contained an updated field value in an unexpected SOAP Notify field.	5 min
EvUdNotifyUpdateFailed	Total number of individual notifications within a SOAP Notify request which were valid, resulted in the subscriber Profile needing to be updated, but the Profile failed to be updated.	5 min
EvUdReSearchDeleteFailed	Total number of LDAP Search requests for re-reading a subscriber which indicated that the subscriber was unknown on the Ud Server, and the subscriber failed to be deleted.	5 min
EvUdReSearchProfileUpdateFailed	Total number of LDAP Search requests for re-reading a subscriber where the returned data was different to the existing subscriber data thus requiring a subscriber Profile update, and the subscriber Profile update failed.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
EvUdSearchCannotSend	Total number of times an attempt to send an LDAP Search request has failed because no LDAP connection was available to send it upon.	5 min
EvUdShCreateSubFailed	Total number of failed attempts to create an auto-enrolled subscriber via the Sh interface.	5 min
EvUdSOAPIdleConnectionDropped	Total number of times a SOAP connection has been disconnected after requests have been sent, but no data has been received within the configured time period.	5 min
EvUdSOAPTCPSendBufferFull	Total number of times an attempt to send a SOAP Subscribe request on a connection has failed because the TCP/IP send buffer is full.	5 min
EvUdSubscribeCannotSend	Total number of times an attempt to send a SOAP Search request has failed because no SOAP connection was available to send it upon.	5 min
EvUdSubscribeDeleteFailed	Total number of Ud Subscribe requests which resulted in an "Unknown Subscriber" response, and the subscriber failed to be deleted.	5 min
EvUdSubscribeRequestTimedOut	Total number of SOAP Subscribe requests that timed out before a response was received.	5 min
EvUdSubscribeUpdateFailed	Total number of successful Ud Subscribe attempts where the subscribers "last subscribe time" failed to be updated.	5 min
RxUdBindResponseAuthenticationFailed	Total number of LDAP Bind requests which resulted in a response indicating "Authentication Failed."	5 min
RxUdBindResponseFailed	Total number of LDAP Bind requests which resulted in a response indicating "Failure."	5 min
RxUdNotifyRequestTooMuchData	Total number of SOAP Notify requests received that were too large to process.	5 min
RxUdNotifyRequestInvalidKey	Total number of SOAP Notify requests received that contained a DN/objectClass from which a valid key type could not be deduced.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
RxUdNotifyResponseRequestNotFound	Total number of SOAP Notify responses received by the Ud Client application from the UDR BE where the corresponding SOAP Notify request could not be found in the list of outstanding requests.	5 min
RxUdSearchRequestTimedOut	Total number of LDAP Search requests which timed out before a response was received.	5 min
RxUdSearchResponseAuthenticationFailed	Total number of LDAP Search responses received which indicated "Authentication Failed."	5 min
RxUdSearchResponseRequestNotFound	Total number of LDAP Search responses received where the initiating request could not be found in the list of outstanding requests.	5 min
RxUdSearchResponseTimeout	Total number of LDAP Search responses received which indicated "Timeout."	5 min
RxUdSubscribeResInvldCorrelationHeader	Total number of SOAP Subscribe responses received that contained an invalid correlation header.	5 min
RxUdSubscribeResponseRequestNotFound	Total number of SOAP Subscribe responses received where the initiating request could not be found in the list of outstanding requests.	5 min
TxUdNotifyResponseSendFailed	Total number of SOAP Notify responses received which failed to be send on the SOAP connection.	5 min
TxUdrBeUdSearchRequestSendFailed	Total number of Ud Search requests that failed to be sent from the UDR BE to the Ud Client application.	5 min
TxUdrBeUdUnsubscribeRequestSendFailed	Total number of Ud Subscribe requests to unsubscribe that failed to be sent from the UDR BE to the Ud Client application.	5 min
TxUdBindRequestSendFailed	Total number of LDAP Bind requests which failed to be sent.	5 min
TxUdReSearchFailedInitiate	Total number of Ud Subscribe requests that failed to be sent from the UDR BE to the Ud Client application.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
TxUdReSubscribeFailedInitiate	Total number of Ud Subscribe requests that failed to be sent from the Ud-Created Audit task to the Ud Client application.	5 min
TxUdReSubscribeFailedNoValidKey	Total number of LDAP Search requests for re-reading a subscriber which could not be sent, because the subscriber Profile did not contain a key that could be mapped to a valid Search DN/filter.	5 min
TxUdSearchRequestSendBufferFull	Total number of times an attempt to send an LDAP Search request on a connection has failed because the TCP/IP send buffer is full.	5 min
TxUdSubscribeRequestSendBufferFull	Total number of SOAP Subscribe requests that failed to be sent due to the TCP/IP send buffer being full.	5 min
TxUdSubscribeRequestSendFailed	Total number of SOAP Subscribe requests that failed to be sent due to another error than the TCP/IP send buffer being full.	5 min
Ud LDAP Interface		
EvUdBindRequest	Total number of LDAP Bind requests attempted to be sent	5 min
EvUdLDAPConnectionBusy	Total number of times an attempt to send an LDAP Search request has failed because a "Busy" error has been returned.	5 min
EvUdUnbindRequest	Total number of LDAP Unbind requests attempted to be sent.	5 min
RxUdBindResponseSuccess	Total number of LDAP Bind requests which resulted in a successful response.	5 min
RxUdSearchRequest	Total number LDAP Search requests received by the Ud Client application.	5 min
RxUdSearchResponseBusy	Total number of LDAP Search responses received which indicated the Ud Server was busy.	5 min
RxUdSearchResponseFailed	Total number of LDAP Search responses received which indicated "Failed."	5 min
RxUdSearchResponseSuccess	Total number of LDAP Search responses received which indicated "Success."	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
RxUdSearchResponseUnknownSubscriber	Total number of LDAP Search responses received which indicated "Unknown Subscriber."	5 min
TxUdBindRequestSendSuccess	Total number of LDAP Bind requests which were sent successfully.	5 min
TxUdUnbindRequestSent	Total number of LDAP Unbind requests which were sent successfully.	5 min
UDR Client Performance		
EvUdNotifyDeleteSubscriber	Total number of individual notifications within a SOAP Notify request which indicated the deletion of a subscriber.	5 min
EvUdNotifyDeleteSubscriberSuccess	Total number of subscribers indicated as deleted in a SOAP Notify request where the subscriber was successfully deleted.	5 min
EvUdNotifyNoUpdatesMade	Total number of individual notifications within a SOAP Notify request which were valid, but did not result in the subscriber Profile being updated.	5 min
EvUdNotifySubscriberNotUdCreated	Total number of individual notifications within a SOAP Notify request for which the subscriber exists, but was not Ud-Created.	5 min
EvUdNotifyUnknownSubscriber	Total number of individual notifications within a SOAP Notify request for which the subscriber was not found in OCUDR.	5 min
EvUdNotifyUpdateSuccess	Total number of individual notifications within a SOAP Notify request which were valid, resulted in the subscriber Profile needing to be updated, and the Profile was successfully updated.	5 min
EvUdReSearchDeleteSuccess	Total number of LDAP Search requests for re-reading a subscriber which indicated that the subscriber was unknown on the Ud Server, and the subscriber was successfully deleted.	5 min
EvUdReSearchProfileDifferent	Total number of LDAP Search requests for re-reading a subscriber where the returned data was different to the existing subscriber data thus requiring a subscriber Profile update.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
EvUdReSearchProfileSame	Total number of LDAP Search requests for re-reading a subscriber where the returned data was the same as the existing subscriber data thus not requiring a subscriber Profile update.	5 min
EvUdReSearchProfileUpdateSuccess	Total number of LDAP Search requests for re-reading a subscriber where the returned data was different to the existing subscriber data thus requiring a subscriber Profile update, and the subscriber Profile update was successful.	5 min
EvUdSimultaneousAccessReq	Total number of Sh requests that resulted in Ud-Creating a subscribe at the same time as another request also creating the same subscriber.	5 min
EvUdSimultaneousAccessReqProfileDiff	Total number of Sh requests that resulted in Ud-Creating a subscribe at the same time as another request also creating the same subscriber where the subscriber Profile was read again, but was different to existing Profile, resulting in a subscriber Profile update.	5 min
EvUdSimultaneousAccessReqProfileSame	Total number of Sh requests that resulted in Ud-Creating a subscribe at the same time as another request also creating the same subscriber where the subscriber Profile was read again, but was the same as the existing Profile.	5 min
EvUdSubscribeDeleteSuccess	Total number of Ud Subscribe requests which resulted in an "Unknown Subscriber" response, and the subscriber was successfully deleted.	5 min
EvUdSubscribeUpdateSuccess	Total number of successful Ud Subscribe attempts where the subscribers "last subscribe time" was updated successfully.	5 min
RxUdNotifyRequest	Total number of SOAP Notify requests received by the UDR application.	5 min
RxUdrBeUdSearchResponseReceived	Total number of Ud Search responses received by the UDR BE.	5 min
RxUdrBeUdSubscribeResponseReceived	Total number of Ud Subscribe responses received by the UDR BE.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
RxUdReSearchBusy	Total number of LDAP Search requests for re-reading a subscriber which failed due to a "Busy" error.	5 min
RxUdReSearchFailed	Total number of LDAP Search requests for re-reading a subscriber which failed due to an error other than "Busy" or "Unknown Subscriber."	5 min
RxUdReSearchUnknownSubscriber	Total number of LDAP Search requests for re-reading a subscriber which indicated that the subscriber was unknown on the Ud Server.	5 min
RxUdShCreateSubSuccess	Total number of Ud-Created subscribers created via the Sh interface.	5 min
RxUdShPurCreateMsgs	Total number of PUR requests received via the Sh interface where the subscriber was unknown and Ud-Creation was triggered to create the subscriber.	5 min
RxUdShSnrCreateMsgs	Total number of SNR requests received via the Sh interface where the subscriber was unknown and Ud-Creation was triggered to create the subscriber.	5 min
RxUdShUdrCreateMsgs	Total number of UDR requests received via the Sh interface where the subscriber was unknown and Ud-Creation was triggered to create the subscriber.	5 min
TxUdNotifyResponseSent	Total number of Ud Notify responses sent to the Ud Client application.	5 min
TxUdrBeUdSearchRequestSent	Total number of Ud Search requests sent triggered by the initial Ud-Creation of a subscriber.	5 min
TxUdrBeUdUnsubscribeRequestSent	Total number of Ud Subscribe requests to unsubscribe triggered by a provisioning request to delete a subscriber.	5 min
TxUdReSearchSendSearch	Total number of Ud Search requests sent upon re-reading a Ud-Created subscriber.	5 min
TxUdReSearchSendThrottled	Total number of Ud Search requests that were attempted to be sent as part of a re-read, but were not sent due to throttling of re-read requests.	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
TxUdReSubscribeSendSubscribe	Total number of Ud Subscribe requests sent upon re-subscribing a Ud-Created subscriber.	5 min
TxUdSearchRequestSent	Total number of LDAP Search requests sent on the LDAP interface.	5 min
TxUdSubscribeRequestInitialSent	Total number of Ud Subscribe requests sent triggered by the initial Ud-Creation of a subscriber.	5 min
TxUdSubscribeRequestSent	Total number of Ud Subscribe requests sent on the SOAP interface.	5 min
Ud SOAP Interface		
EvUdSOAPConnectionBusy	Total number of times an attempt to send a SOAP Subscribe request has failed because a "Busy" error has been returned.	5 min
RxUdNotifyRequestBusy	Total number of SOAP Notify requests rejected because OCUDR was too busy.	5 min
RxUdNotifyRequestDiscarded	Total number of SOAP Notify requests received without a SOAP header.	5 min
RxUdNotifyRequestInvalidRequest	Total number of SOAP Notify requests received that did not comply to the expected format.	5 min
RxUdNotifyRequestReceived	Total number of SOAP Notify requests received by the SOAP Interface.	5 min
RxUdNotifyRequestValid	Total number of SOAP Notify requests that were sent by the Ud Client application to the UDR BE.	5 min
RxUdNotifyResponseBusy	Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Busy."	5 min
RxUdNotifyResponseFailed	Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Failed."	5 min
RxUdNotifyResponseInvalidRequest	Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Invalid Request."	5 min

Table 5-7 (Cont.) Ud Client Measurements

Measurement Tag	Description	Collection Interval
RxUdNotifyResponseSuccess	Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Success."	5 min
RxUdNotifyResponseUnknownSubscriber	Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Unknown Subscriber."	5 min
RxUdSubscribeRequest	Total number SOAP Subscribe requests received by the Ud Client application.	5 min
RxUdSubscribeResponseFailed	Total number of SOAP Subscribe responses received which indicated "Failed."	5 min
RxUdSubscribeResponseReceived	Total number of SOAP Subscribe responses received.	5 min
RxUdSubscribeResponseSuccess	Total number of SOAP Subscribe responses received which indicated "Success."	5 min
RxUdSubscribeResponseUnknownSubscriber	Total number of SOAP Subscribe responses received which indicated "Unknown Subscriber."	5 min
RxUdUnsubscribeRequest	Total number SOAP Unsubscribe requests received by the Ud Client application.	5 min
TxUdSubscribeRequestSubscribeSent	Total number of SOAP Subscribe requests which indicate a request to "subscribe" to subscriber data change notifications that were successfully sent.	5 min
TxUdSubscribeRequestUnsubscribeSent	Total number of SOAP Subscribe requests which indicate a request to "unsubscribe" to subscriber data change notifications that were successfully sent.	5 min

Ud Client Exceptions

EvUdBindRequestTimedOut

Measurement ID
3893

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Bind requests which timed out before a response was received.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Bind request on an LDAP connection was successfully sent, but no response was received in the configured time period.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdLDAPIdleConnectionDropped

Measurement ID
3908

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
The measurement shall be incremented each time an LDAP connection has been marked congested due to the TCP/IP send buffer being full, no LDAP Search requests can be successfully sent, and no responses are have been received for a configured period, resulting in the connection being dropped.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP connection has been marked congested due to the TCP/IP send buffer being full, no LDAP Search requests can be successfully sent, and no responses are have been received for a configured period, resulting in the connection being dropped.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdLDAPTCPSendBufferFull

Measurement ID
3909

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of times an attempt to send an LDAP Search request on a connection has failed because the TCP/IP send buffer is full.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP Search request on an LDAP connection fails because the TCP/IP send buffer is full.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyDeleteSubscriberFailed

Measurement ID
3925

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of subscribers indicated as deleted in a SOAP Notify request where the subscriber failed to be deleted.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received which indicates that the subscriber has been deleted in the Ud Server, and the subscriber failed to be deleted in OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyFieldUpdateFailure

Measurement ID
3926

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request which attempted to update a field to an invalid value according to the field definition in the SEC.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP attribute included in a SOAP Notify request fails field validation as defined in the SEC, resulting in the individual notification being rejected.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyRequestTimeout

Measurement ID
3978

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests that were sent by the Ud Client application to the UDR BE for which no response was received within the expected time period.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application does not receive a response to a notify request sent to the UDR application within the configured timeout period.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyUnexpectedUpdateField

Measurement ID
3927

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request which contained an updated field value in an unexpected SOAP Notify field.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an unexpected notification update field is encountered in a SOAP Notify request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyUpdateFailed

Measurement ID
3930

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request which were valid, resulted in the subscriber Profile needing to be updated, but the Profile failed to be updated.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a notification is processed and subscriber Profile fields have change, and the update of the subscriber Profile failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdReSearchDeleteFailed

Measurement ID
3941

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which indicated that the subscriber was unknown on the Ud Server, and the subscriber failed to be deleted.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request returned an error indicating the subscriber was not known on the Ud Server, and the subscriber failed to be deleted in OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdReSearchProfileUpdateFailed

Measurement ID
3937

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber where the returned data was different to the existing subscriber data thus requiring a subscriber Profile update, and the subscriber Profile update failed.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request has returned subscriber data, and the subscriber Profile needs to be updated, and the subscriber Profile update failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSearchCannotSend

Measurement ID
3912

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of times an attempt to send an LDAP Search request has failed because no LDAP connection was available to send it upon.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search request cannot be sent because all LDAP connections are either not connected, or in a busy state.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdShCreateSubFailed

Measurement ID
3907

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of failed attempts to create an auto-enrolled subscriber via the Sh interface.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a Ud-Created subscriber fails to be created.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSOAPIdleConnectionDropped

Measurement ID
3913

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of times a SOAP connection has been disconnected after requests have been sent, but no data has been received within the configured time period.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP connection has been marked congested due to the TCP/IP send buffer being full, no SOAP Subscribe requests can be successfully sent, and no responses are have been received for a configured period, resulting in the connection being dropped.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSOAPTCPSendBufferFull

Measurement ID
3914

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of times an attempt to send a SOAP Subscribe request on a connection has failed because the TCP/IP send buffer is full.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send a SOAP Subscribe request on a SOAP connection fails because the TCP/IP send buffer is full.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSubscribeCannotSend

Measurement ID
3912

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of times an attempt to send a SOAP Search request has failed because no SOAP connection was available to send it upon.

Collection Interval:
5 min

Peg Condition:
The measurement shall be incremented each time a SOAP Subscribe request cannot be sent because all SOAP connections are either not connected, or in a busy state.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSubscribeDeleteFailed

Measurement ID
3900

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests which resulted in an "Unknown Subscriber" response, and the subscriber failed to be deleted.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a response to a SOAP Subscribe request has indicated an "Unknown Subscriber" error, and the subscriber failed to be deleted from OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSubscribeRequestTimedOut

Measurement ID
3965

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe requests that timed out before a response was received.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Subscribe request on a SOAP connection was successfully sent, but no response was received in the configured time period.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSubscribeUpdateFailed

Measurement ID
3902

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of successful Ud Subscribe attempts where the subscribers "last subscribe time" failed to be updated.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application receives a failure response to a SOAP Subscribe request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdBindResponseAuthenticationFailed

Measurement ID
3898

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Bind requests which resulted in a response indicating "Authentication Failed."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind request on an LDAP connection that indicated an authentication failure has occurred on the Ud Server.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdBindResponseFailed

Measurement ID
3895

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Bind requests which resulted in a response indicating "Failure."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind request on an LDAP connection that indicated an error other than an authentication failure has occurred on the Ud Server.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestTooMuchData

Measurement ID
3974

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests received that were too large to process.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is larger than the maximum allowed size.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestInvalidKey

Measurement ID
3975

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests received that contained a DN/objectClass from which a valid key type could not be deduced.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request contains an individual notification where the subscriber key cannot be correlated with the keys configured for the LDAP/SOAP interfaces.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyResponseRequestNotFound

Measurement ID
3979

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received by the Ud Client application from the UDR BE where the corresponding SOAP Notify request could not be found in the list of outstanding requests.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a notify response from the UDR application, and the corresponding request is not found in the list of outstanding notify requests.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchRequestTimedOut

Measurement ID
3951

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search requests which timed out before a response was received.

Collection Interval:
5 min

Peg Condition:
The measurement shall be incremented each time an LDAP Search request on an LDAP connection was successfully sent, but no response was received in the configured time period.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseAuthenticationFailed

Measurement ID
3956

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated "Authentication Failed."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind Search on an LDAP connection that indicated an error that maps to the authentication failed status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseRequestNotFound

Measurement ID
3952

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received where the initiating request could not be found in the list of outstanding requests.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time upon receipt of an LDAP Search response on an LDAP connection, the corresponding request is not found in the list of outstanding requests for the LDAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseTimeout

Measurement ID
3958

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated "Timeout."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search request on an LDAP connection was successfully sent, but no response was received in the configured time period.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeResInvIdCorrelationHeader

Measurement ID
3967

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe responses received that contained an invalid correlation header.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Subscribe response does not contain a valid SOAP header, as specified by 3GPP.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeResponseRequestNotFound

Measurement ID
3968

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe responses received where the initiating request could not be found in the list of outstanding requests.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time upon receipt of a SOAP Subscribe response on a SOAP connection, the corresponding request is not found in the list of outstanding requests for the SOAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdNotifyResponseSendFailed

Measurement ID
3985

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received which failed to be send on the SOAP connection.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send a SOAP Notify response on a SOAP connection failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBeUdSearchRequestSendFailed

Measurement ID
3917

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of Ud Search requests that failed to be sent from the UDR BE to the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application fails to send a Search request to the Ud Client application.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBeUdUnsubscribeRequestSendFailed

Measurement ID
3988

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests to unsubscribe that failed to be sent from the UDR BE to the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application fails to send an Unsubscribe request to the Ud Client application.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdBindRequestSendFailed

Measurement ID
3892

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Bind requests which failed to be sent.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP Bind request on an LDAP connection failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdReSearchFailedInitiate

Measurement ID
3934

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests that failed to be sent from the UDR BE to the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt by the UDR application to send an LDAP Search request to the Ud Client application, as part of a re-search request failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdReSubscribeFailedInitiate

Measurement ID
3947

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which could not be sent, because the subscriber Profile did not contain a key that could be mapped to a valid Search DN/filter.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt by the UDR application to send a SOAP Subscribe request to the Ud Client application, as part of a re-subscribe request failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdReSubscribeFailedNoValidKey

Measurement ID
3946

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which could not be sent, because the subscriber Profile did not contain a key that could be mapped to a valid Search DN/filter.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a request to re-subscribe for a subscriber cannot be sent because the subscriber does not have a subscriber Profile key value which is configured for use on the SOAP/LDAP interface for the Ud Client.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSearchRequestSendBufferFull

Measurement ID
3950

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of times an attempt to send an LDAP Search request on a connection has failed because the TCP/IP send buffer is full.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application attempts to send an LDAP Search request, and upon sending, detects that the TCP/IP send buffer for the connection is full.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSubscribeRequestSendBufferFull

Measurement ID
3963

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe requests which indicate a request to "subscribe" to subscriber data change notifications that were successfully sent. Total number of SOAP Subscribe requests that failed to be sent due to the TCP/IP send buffer being full.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application attempts to send a SOAP Subscribe request, and upon sending, detects that the TCP/IP send buffer for the connection is full.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSubscribeRequestSendFailed

Measurement ID
3964

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe requests that failed to be sent due to another error than the TCP/IP send buffer being full.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send a SOAP Subscribe request on a SOAP connection failed.

Measurement Scope:
Server Group

Recovery:

1. No action required.

Ud LDAP Interface

EvUdBindRequest

Measurement ID
3890

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP bind requests attempted to be sent.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP bind request is made on an LDAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdLDAPConnectionBusy

Measurement ID
3910

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of times an attempt to send an LDAP Search request has failed because a "Busy" error has been returned.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response is received indicating a "Busy" status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdUnbindRequest

Measurement ID
3896

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Unbind requests attempted to be sent.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP Unbind request is made on an LDAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdBindResponseSuccess

Measurement ID
3994

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Bind requests which resulted in a successful response.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a successful response was received for an LDAP Bind request on an LDAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchRequest

Measurement ID
3948

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number LDAP Search requests received by the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a request from the UDR application to send an LDAP Search request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseBusy

Measurement ID
3957

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated the Ud Server was busy.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind Search on an LDAP connection that indicated an error that maps to the authentication failed status The measurement shall be incremented each time an error response was received for an LDAP Bind Search on an LDAP connection that indicated an error that maps to the busy status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseFailed

Measurement ID
3955

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated "Failed."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind Search on an LDAP connection that indicated an error that maps to the failed status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseSuccess

Measurement ID
3953

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated "Success."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a successful response was received for an LDAP Search request on an LDAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseUnknownSubscriber

Measurement ID
3954

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated "Unknown Subscriber."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Search request on an LDAP connection that indicated the subscriber was unknown on the Ud Server.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdBindRequestSendSuccess

Measurement ID
3891

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Bind requests attempted to be sent.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP Bind request on an LDAP connection was successful.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdUnbindRequestSent

Measurement ID
3897

Measurement Group:
Ud Client LDAP Interface

Measurement Type:
Simple

Description:
Total number of LDAP Unbind requests which were sent successfully.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP Unbind request on an LDAP connection was successful.

Measurement Scope:
Server Group

Recovery:

1. No action required.

UDR Client Performance

EvUdNotifyDeleteSubscriber

Measurement ID
3923

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request which indicated the deletion of a subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received which indicates that the subscriber has been deleted in the Ud Server.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyDeleteSubscriberSuccess

Measurement ID
3924

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of subscribers indicated as deleted in a SOAP Notify request where the subscriber was successfully deleted.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received which indicates that the subscriber has been deleted in the Ud Server, and the subscriber was successfully deleted in OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyNoUpdatesMade

Measurement ID
3928

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request which were valid, but did not result in the subscriber Profile being updated.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time upon successfully completing the processing of a notification, if no subscriber Profile fields were changed (for any reason).

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifySubscriberNotUdCreated

Measurement ID
3922

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request for which the subscriber exists, but was not Ud-Created.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received, and the subscriber exists in OCUDR, but was not Ud-Created.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyUnknownSubscriber

Measurement ID
3921

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request for which the subscriber was not found in OCUDR.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received, and the subscriber does not exist in OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdNotifyUpdateSuccess

Measurement ID
3929

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of individual notifications within a SOAP Notify request which were valid, resulted in the subscriber Profile needing to be updated, and the Profile was successfully updated.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a notification is processed and subscriber Profile fields have change, and the update of the subscriber Profile was successful.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdReSearchDeleteSuccess

Measurement ID
3940

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which indicated that the subscriber was unknown on the Ud Server, and the subscriber was successfully deleted.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request returned an error indicating the subscriber was not known on the Ud Server, and the subscriber was successfully deleted in OCUDR

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdReSearchProfileDifferent

Measurement ID
3935

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber where the returned data was different to the existing subscriber data thus requiring a subscriber Profile update.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request has returned subscriber data, and the subscriber Profile needs to be updated as it is different.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdReSearchProfileSame

Measurement ID
3939

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber where the returned data was the same as the existing subscriber data thus not requiring a subscriber Profile update.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request has returned subscriber data, and the subscriber Profile does not need to be updated as it is the same.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdReSearchProfileUpdateSuccess

Measurement ID
3936

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber where the returned data was different to the existing subscriber data thus requiring a subscriber Profile update, and the subscriber Profile update was successful.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request has returned subscriber data, and the subscriber Profile needs to be updated, and the subscriber Profile update was successful.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSimultaneousAccessReq

Measurement ID
3918

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Sh requests that resulted in Ud-Creating a subscribe at the same time as another request also creating the same subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a request to create a Ud-Created subscriber encounters a situation where the subscriber was also being created at the same time, triggered by a different Sh request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSimultaneousAccessReqProfileDiff

Measurement ID
3920

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Sh requests that resulted in Ud-Creating a subscribe at the same time as another request also creating the same subscriber where the subscriber Profile was read again, but was different to existing Profile, resulting in a subscriber Profile update.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a request to create a Ud-Created subscriber encounters a situation where the subscriber was also being created at the

same time, and the subscriber data retrieved via LDAP for the request was found to be different to the data used to initially create the subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSimultaneousAccessReqProfileSame

Measurement ID
3919

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Sh requests that resulted in Ud-Creating a subscribe at the same time as another request also creating the same subscriber where the subscriber Profile was read again, but was the same as the existing Profile.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a request to create a Ud-Created subscriber encounters a situation where the subscriber was also being created at the same time, and the subscriber data retrieved via LDAP for the request was found to be the same as the data used to initially create the subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSubscribeDeleteSuccess

Measurement ID
3899

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests which resulted in an "Unknown Subscriber" response, and the subscriber was successfully deleted.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a response to a SOAP Subscribe request has indicated an "Unknown Subscriber" error, and the subscriber has been successfully deleted from OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

EvUdSubscribeUpdateSuccess

Measurement ID
3901

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of successful Ud Subscribe attempts where the subscribers "last subscribe time" was updated successfully.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application receives a successful response to a SOAP Subscribe request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequest

Measurement ID
3972

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests received by the UDR application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received by the UDR application.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBeUdSearchResponseReceived

Measurement ID
3990

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Search responses received by the UDR BE.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application receives a response to a Ud Search request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdrBeUdSubscribeResponseReceived

Measurement ID
3991

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud subscribe responses received by the UDRBE.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application receives a response to a Ud subscribe request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdReSearchBusy

Measurement ID
3942

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which failed due to a "Busy" error.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request returned an error indicating that the Ud Server was busy.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdReSearchFailed

Measurement ID
3943

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which failed due to an error other than "Busy" or "Unknown Subscriber".

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request returned an error indicating other than busy or unknown subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdReSearchUnknownSubscriber

Measurement ID
3938

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of LDAP Search requests for re-reading a subscriber which indicated that the subscriber was unknown on the Ud Server.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search response performed as part of a re-search request returned an error indicating the subscriber was not known on the Ud Server.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdShCreateSubSuccess

Measurement ID
3906

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud-Created subscribers created via the Sh interfac.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a Ud-Created subscriber is successfully created.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdShPurCreateMsgs

Measurement ID
3904

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
The total number of PUR requests received via the Sh interface where the subscriber was unknown and Ud-Creation was triggered to create the subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR Back End is processing an update request, the subscriber user identity is not found in the index, and the update request matches Ud-Creation requirements.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdShSnrCreateMsgs

Measurement ID
3905

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of SNR requests received via the Sh interface where the subscriber was unknown and Ud-Creation was triggered to create the subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR Back End is processing a subscribe request, the subscriber user identity is not found in the index, and the read request matches Ud-Creation requirements.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdShUdrCreateMsgs

Measurement ID
3903

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of UDR requests received via the Sh interface where the subscriber was unknown and Ud-Creation was triggered to create the subscriber.

Collection Interval:
5 min

Peg Condition:
This measurement is incremented each time the UDR Back End is processing a subscribe request. The subscriber user identity is not found in the index, and the subscribe request matches Ud-Creation requirements.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdNotifyResponseSent

Measurement ID
3931

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Notify responses sent to the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the UDR application sends a response to a SOAP Notify request to the Ud Client application.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBeUdSearchRequestSent

Measurement ID
3916

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Search requests sent triggered by the initial Ud-Creation of a subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time shall an LDAP Search request is sent during the initial creation of a Ud-Created subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBeUdUnsubscribeRequestSent

Measurement ID
3987

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud unsubscribe requests sent, triggered by a provisioning request to delete a subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time UDR fails to send an unsubscribe request to the Ud client.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdReSearchSendSearch

Measurement ID
3933

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Search requests sent upon re-reading a Ud-Created subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an LDAP Search request is sent as part of a periodic re-search request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdReSearchSendThrottled

Measurement ID
3932

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Search requests that were attempted to be sent as part of a re-read, but were not sent due to throttling of re-read requests.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send an LDAP Search request as part of a re-search request was not sent due to throttling of re-search requests.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdReSubscribeSendSubscribe

Measurement ID
3945

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests sent upon re-subscribing a Ud-Created subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Subscribe request is sent during the re-subscribe of a Ud-Created subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdrBeUdSearchRequestSent

Measurement ID
3916

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Search requests sent triggered by the initial Ud-Creation of a subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time shall an LDAP Search request is sent during the initial creation of a Ud-Created subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSubscribeRequestInitialSent

Measurement ID
3944

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests sent triggered by the initial Ud-Creation of a subscriber.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Subscribe request is sent during the initial creation of a Ud-Created subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSubscribeRequestSent

Measurement ID
3944

Measurement Group:
Ud Client Performance

Measurement Type:
Simple

Description:
Total number of Ud Subscribe requests sent on the SOAP interface.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application has successfully sent a SOAP Subscribe request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

Ud SOAP Interface

EvUdSOAPConnectionBusy

Measurement ID
3915

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of times an attempt to send a SOAP Subscribe request has failed because a "Busy" error has been returned.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Subscribe response is received indicating a "Busy" status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestBusy

Measurement ID
3976

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests rejected because OCUDR was too busy.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received, and OCUDR is too busy to process the request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestDiscarded

Measurement ID
3992

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests received without a SOAP header.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received without a SOAP header.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestInvalidRequest

Measurement ID
3973

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests received that did not comply to the expected format.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify does not contain a valid request, as specified by 3GPP.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestReceived

Measurement ID
3986

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a SOAP Notify request is received on the SOAP interface.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyRequestValid

Measurement ID
3977

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify requests that were sent by the Ud Client application to the UDR BE.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a valid SOAP Notify request is received.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyResponseBusy

Measurement ID
3982

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Busy."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a notify response from the UDR application indicating that the UDR application was too busy to process the request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyResponseFailed

Measurement ID
3983

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Failed."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a notify response from the UDR application indicating a failed response.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyResponseInvalidRequest

Measurement ID
3984

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Invalid Request."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a notify response from the UDR application indicating that the notification was invalid.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyResponseSuccess

Measurement ID
3980

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Success."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a successful notify response from the UDR application.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdNotifyResponseUnknownSubscriber

Measurement ID
3981

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Notify responses received by the Ud Client application from the UDR BE indicating the result "Unknown Subscriber."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a notify response from the UDR application indicating that the subscriber was unknown in OCUDR.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSearchResponseAuthenticationFailed

Measurement ID
3956

Measurement Group:
Ud Client Exception

Measurement Type:
Simple

Description:
Total number of LDAP Search responses received which indicated "Authentication Failed."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind Search on an LDAP connection that indicated an error that maps to the authentication failed status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeRequest

Measurement ID
3959

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number SOAP Subscribe requests received by the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement in incremented each time the Ud Client application receives a request from the UDR application to send a "SOAP Subscribe" request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeResponseFailed

Measurement ID
3971

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe responses received which indicated "Failed."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for an LDAP Bind Search on an LDAP connection that indicated an error that maps to the failed status.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeResponseReceived

Measurement ID
3966

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe responses received.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a response is received for a SOAP Subscribe request on a SOAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeResponseSuccess

Measurement ID
3969

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe responses received which indicated "Success."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time a successful response was received for a SOAP Subscribe request on a SOAP connection.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdSubscribeResponseUnknownSubscriber

Measurement ID
3970

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe responses received which indicated "Unknown Subscriber."

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an error response was received for a SOAP Subscribe request on a SOAP connection that indicated the subscriber was unknown on the Ud Server.

Measurement Scope:
Server Group

Recovery:

1. No action required.

RxUdUnsubscribeRequest

Measurement ID
3989

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number SOAP Unsubscribe requests received by the Ud Client application.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time the Ud Client application receives a request from the UDR application to send a SOAP Subscribe unsubscribe request.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSubscribeRequestSubscribeSent

Measurement ID
3961

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe requests which indicate a request to "subscribe" to subscriber data change notifications that were successfully sent.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send a SOAP Subscribe request on a SOAP connection was successful, and the request was to subscribe to subscribe data change notifications for a subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

TxUdSubscribeRequestUnsubscribeSent

Measurement ID
3962

Measurement Group:
Ud Client SOAP Interface

Measurement Type:
Simple

Description:
Total number of SOAP Subscribe requests which indicate a request to "subscribe" to subscriber data change notifications that were successfully sent Total number of SOAP Subscribe requests which indicate a request to "unsubscribe" to subscriber data change notifications that were successfully sent.

Collection Interval:
5 min

Peg Condition:
The measurement is incremented each time an attempt to send a SOAP Subscribe request on a SOAP connection was successful, and the request was to subscribe to unsubscribe from data change notifications for a subscriber.

Measurement Scope:
Server Group

Recovery:

1. No action required.

Index

A

E