Oracle® Communications Diameter Signaling Router

Alarms, KPIs, and Measurements Reference

910-6922-001 Revision A

May 2014

ORACLE®

Oracle® Communications Alarms, KPIs, and Measurements Reference

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

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

Overview

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

This documentation provides:

- 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
- Information relevant to understanding KPIs in the application
- The procedure for viewing KPIs
- Lists of KPIs
- Information relevant to understanding measurements in the application
- Measurement report elements, and the procedures for printing and exporting measurements
- Lists of measurements by function

Scope and Audience

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

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

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

Manual Organization

Information in this document is organized into the following sections:

- *Introduction* contains general information about this document, how to contact the *Customer Care Center*, and *Locate Product Documentation on the Customer Support Site*.
- *Alarms and Events, KPIs, and Measurements Overview* provides general information about the application's alarms and events, KPIs, and measurements.
- *Alarms and Events* provides information and recovery procedures for alarms and events, organized first by alarm category, then numerically by the number that appears in the application.
- *Key Performance Indicators (KPIs)* provides detailed KPI information, organized alphabetically by KPI name.
- *Measurements* provides detailed measurement information, organized alphabetically by measurement category.

- *Policy DRA Error Resolution Procedures* provides information regarding various error codes associated with Policy DRA.

Documentation Admonishments

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

Table 1: Admonishments

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

Related Publications

The Diameter Signaling Router (DSR) documentation set includes the following publications, which provide information for the configuration and use of DSR and related applications.

Getting Started includes a product overview, system architecture, and functions. It also explains the DSR GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

Feature Notice describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Oracle Customer Support Site.

Roadmap to Hardware Documentation provides links to access manufacturer online documentation for hardware related to the DSR.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the DSR, both for initial setup and maintenance.

Communication Agent User's Guide explains how to use the Communication Agent GUI pages to configure Remote Servers, Connection Groups, and Routed Servers, and to maintain configured connections.

Diameter and Mediation User's GuideDiameter User's Guide explains how to use the Diameter GUI pages to manage the configuration and maintenance of Diameter Configuration components, including Local and Peer Nodes, Connections, Configuration Sets, Peer Routing Rules, Application Route Tables, System Options, and DNS options; describes the functions of Diameter Message Copy; explains how to configure and use Diameter Mediation; and describes DSR capacity and congestion controls.

Diameter Mediation User's Guide describes the functions of Diameter Mediation, and explains how to use the Diameter Mediation GUI pages (nested inside the Diameter GUI folder) to configure and test Rule Templates, how to use the Formatting Value Wizard, and how to configure Rule Sets.

IP Front End (IPFE) User's Guide explains how to the use the IPFE GUI pages to configure IPFE to distribute IPv4 and IPv6 connections from multiple clients to multiple nodes.

Range-Based Address Resolution (RBAR) User's Guide explains how to use the RBAR GUI pages to configure RBAR to route Diameter end-to-end transactions based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges and individual addresses.

Full-Address Based Resolution (FABR) User's Guide explains how to use the FABR GUI pages to configure FABR to resolve designated Diameter server addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses.

Charging Proxy Application (CPA) and Offline Charging Solution User's Guide describes the Offline Charging Solution and explains how to use the CPA GUI pages to set System Options for CPA, configure the CPA's Message Copy capability, and configure the Session Binding Repository for CPA.

Policy DRA User's Guide describes the topology and functions of the Policy Diameter Routing Agent (Policy DRA) DSR Application and the Policy Session Binding Repository, and explains how to use the GUI pages to configure Policy DRA.

Gateway Location Application (GLA) User's Guide describes the functions of retrieving subscriber data stored in Policy Session Binding Repository (pSBR) provided by Policy DRA and explains how to use the GUI pages to configure GLA.

DSR Alarms, KPIs, and Measurements Reference provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual Diameter measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

DSR Administration Guide describes DSR architecture, functions, configuration, and tools and utilities (IPsec, Import/Export, DIH, and database backups); and provides references to other publications for more detailed information.

Customer Care Center

Oracle's Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your

requests to the Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Technical Assistance Centers are located around the globe in the following locations:

Related - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

01-800-912-0537

- **Dominican Republic**

  Phone:

  1-888-367-8552

- **Mexico**

  Phone:

  001-888-367-8552

- **Peru**

  Phone:

  0800-53-087

- **Puerto Rico**

  Phone:

  1-888-367-8552

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**

Phone:

+65 6796 2288

TAC Regional Support Office Hours:

9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by Oracle's Tekelec Customer Care Center 24 hours a day, 7 days a week. 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's Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

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

1. Log into the Oracle Customer Support site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter

2

Alarms and Events, KPIs, and Measurements Overview

Topics:

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

Displaying the file list

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

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

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

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

Data Export

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

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

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

Data Export elements

This table describes the elements on the Data Export page.

Table 2: Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server.	Must be a valid hostname, IPv4 address, or IPv6 address. Range: Maximum length is 24 characters; alphanumeric characters (a-z, A-Z, and 0-9) and minus sign. Hostname must start and end with an alphanumeric. To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None

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

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

Configuring data export

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

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

14. Click **OK** or **Apply**.
    The export server is now configured and available to receive performance and configuration data.

Tasks

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

Active Tasks

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

Active Tasks elements

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

Table 3: Active Tasks Elements

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

Deleting a task

Use this procedure to delete one or more tasks.

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

The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.
3. Select one or more tasks.

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

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

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK** to delete the selected task(s).
   The selected task(s) are deleted from the table.

Deleting all completed tasks

Use this procedure to delete all completed tasks.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.
3. Click **Delete all Completed**.
   A confirmation box appears.
4. Click **OK** to delete all completed tasks.
   All tasks with the status of completed are deleted.

Canceling a running or paused task

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

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.
3. Select a task.
4. Click **Cancel**.
   A confirmation box appears.
5. Click **OK** to cancel the selected task.

The selected task is canceled.

Pausing a task

Use this procedure to pause a task.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select a task.

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

4. Click **Pause**.
   A confirmation box appears.
5. Click **OK** to pause the selected task.
   The selected task is paused. For information about restarting a paused task, see *Restarting a task*.

Restarting a task

Use this procedure to restart a task.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select a paused task.

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

4. Click **Restart**.
   A confirmation box appears.
5. Click **OK** to restart the selected task.
   The selected task is restarted.

Active Tasks report elements

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

Table 4: Active Tasks Report Elements

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

Generating an active task report

Use this procedure to generate an active task report.

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

   The **Active Tasks** page appears.

2. Select a server.

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

   All active tasks on the selected server are displayed.

3. Select one or more tasks.

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

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

Scheduled Tasks

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

- *Exporting active alarms*

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

Viewing scheduled tasks

Use this procedure to view the scheduled tasks.

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

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

Scheduled Tasks elements

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

Table 5: Scheduled Tasks Elements

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

Editing a scheduled task

Use this procedure to edit a scheduled task.

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

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

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

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

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

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

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

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

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

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

2. Select one or more tasks.

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

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

Chapter 3

Alarms and Events

Topics:

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

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

General alarms and events information

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

Alarms and events overview

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

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

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

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

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

The following figure shows how Alarms and Events are organized in the application.

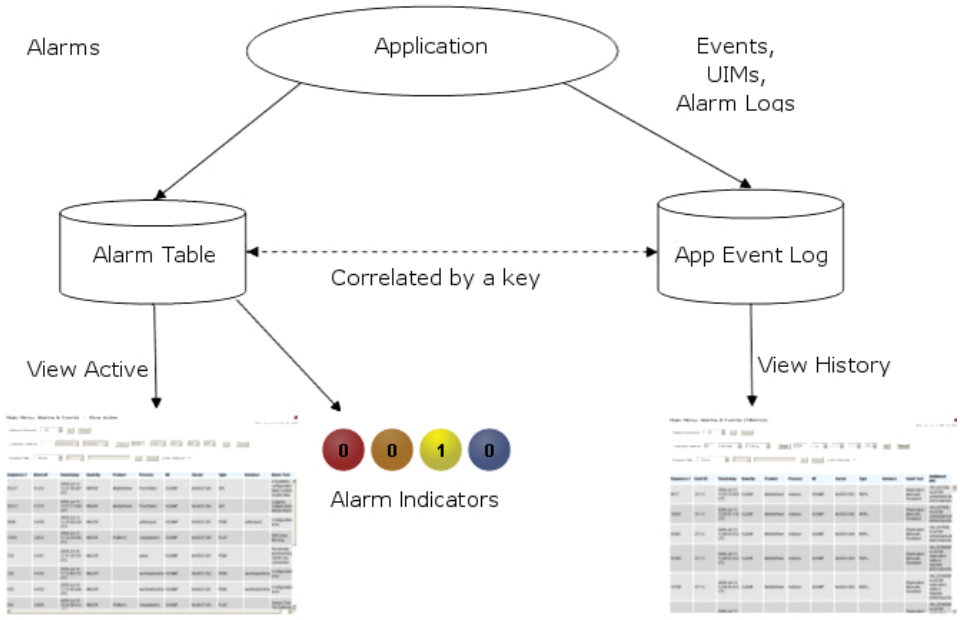


Figure 1: Flow of Alarms

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.

●	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 2: Alarm Indicators Legend

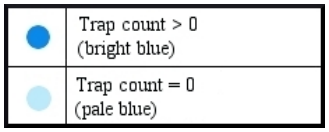


Figure 3: Trap Count Indicator Legend

Alarms formatting information

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

The information provided about each alarm includes:

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

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

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

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

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

Alarm and event ID ranges

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

Table 6: Alarm/Event ID Ranges

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

Application/Process Name	Alarm ID Range
FABR	22600-22640
PDRA	22700-22799
CPA	22800-22849
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32700
GLA	33100-33149

Alarm and event types

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

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

Table 7: Alarm and Event Types

Type Name	Type
APPL	Application
CAF	Communication Agent (ComAgent)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
CHG	Charging
CNG	Congestion Control
COLL	Collection
CPA	Charging Proxy Application
DB	Database
DIAM	Diameter
DISK	Disk
DNS	Domain Name Service
DPS	Data Processor Server
ERA	Event Responder Application
FABR	Full Address Based Resolution
HA	High Availability

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

Viewing active alarms

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

Use this procedure to view active alarms.

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

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

   The active alarms table updates automatically. When new alarms are generated, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.
   The following message appears: `(Alarm updates are suspended.)`

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

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

Active alarms data export elements

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

Table 8: Schedule Active Alarm Data Export Elements

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

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

Exporting active alarms

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

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

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

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

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

1. Select **Alarms & Events > View Active**.
   The **View Active** page appears.
2. If necessary, specify filter criteria and click **Go**.
   The active alarms are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule Active Alarm Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *Active alarms data export elements* .

5. Select the **Export Frequency**.
6. Select the **Time of Day**.

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

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

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

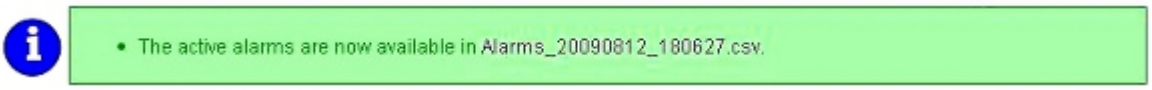
8. Click **OK** or **Apply** to initiate the active alarms export task.

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

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

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

9. Click **Export**.
   The file is exported.
10. Click the link in the green message box to go directly to the **Status & Manage > Files** page.



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

Generating a report of active alarms

Use this procedure to generate a report.

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

   The **View Active** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The active alarms are displayed according to the specified criteria. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.
3. Click **Report**.
   The View Active Report is generated. This report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Viewing alarm and event history

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

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

1. Select **Alarms & Events > View History** .
   The **View History** page appears.
2. If necessary, specify filter criteria and click **Go**.

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

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

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

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

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

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

Historical events data export elements

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

Table 9: Schedule Event Data Export Elements

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

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

Exporting alarm and event history

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

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

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

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

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

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

5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes.**
7. Select the **Time of Day**.

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

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

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

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

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

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

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

10. Click **Export**.
    The file is exported.
11. Click the link in the green message box to go directly to the **Status & Manage > Files** page.

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

Generating a report of historical alarms and events

Use this procedure to generate a report.

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

   The **View History** page appears.

2. Specify filter criteria, if necessary, and click **Go**.
   The historical alarms and events are displayed according to the specified criteria.
3. Click **Report**.
   The View History Report is generated. This report can be printed or saved to a file.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

IP Front End, IPFE (5000-5999)

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

5001 - IPFE Backend Unavailable

Alarm Type: IPFE

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

Severity: Minor

Instance: IP address of the application server

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendUnavailableNotify

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

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

5002 - IPFE address configuration error

Alarm Type: IPFE

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

Severity: Critical

Instance: One of the following strings:

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

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeStateSyncConfigErrorNotify

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

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

   The **Configuration Options** pane appears.

2. Ensure that **IPFE1 IP Address** and **IPFE2 IP Address** are configured correctly.
3. For issues with modules or versions, contact the *Customer Care Center* for assistance.

5003 - IPFE state sync run error

Alarm Type: IPFE

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

Severity: Critical

Instance: One of the following strings:

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

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeStateSyncRunErrorNotify

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

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

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

   4. Click **OK** to continue.
3. Diagnose any network fault between the two IPFEs.
4. For further assistance, contact the *Customer Care Center*.

5004 - IPFE IP tables configuration error

Alarm Type: IPFE

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeIpTablesConfigErrorNotify

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

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

   The **Configuration Options** pane appears.

2. Ensure that the **TSA1 IP Address** field contains a valid IP address.
3. Select **IPFE > Configuration > IP List TSA 1**.

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

4. Ensure that there is at least one application server IP address configured for the TSA.
5. Repeat for **IPFE > Configuration > IP List TSA 1**.

5005 - IPFE Backend In Stasis

Alarm Type: IPFE

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

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

Severity: Minor

Instance: IP address of the application server in stasis

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendInStasisNotify

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

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

Alarm Type: IPFE

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

Severity: Critical

Instance: "pcap <ethernet device name>"

HA Score: Degraded

Auto Clear Seconds: N/A

OID: ipfeIpfeEtherDeviceReadError

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

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

   A warning message appears:

   Are you sure you want to restart application software on the following server(s)? <server name>
4. Click **OK** to continue.

5007 - Out of Balance: Low

Alarm Type: IPFE

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

Severity: Minor

Instance: IP address of the application server

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendUnderloadedNotify

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

5008 - Out of Balance: High

Alarm Type: IPFE

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

Severity: Minor

Instance: IP address of the overloaded application server

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeBackendOverloadedNotify

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

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

5009 - No available servers in target set

Alarm Type: IPFE

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeNoAvailableAppServersNotify

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

1. Ensure that application servers have been configured for the target set address by viewing **IPFE > Configuration > Target Sets**.
2. Check the status of the application servers by navigating to the **Status & Manage > Server** page.
3. Consult the application server's documentation for recovery steps.
4. Ensure that `ipfeNetUpdate.sh` has been run by looking for the following lines in `/etc/sysconfig/` network on the IPFE blades:

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

   If `ipfeNetUpdate.sh` has not bee run:

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

5. If application servers have been configured correctly for the target set and the application server status is healthy, contact the *Customer Care Center* for assistance.

5010 - Unknown Linux iptables command error

Alarm Type: IPFE

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

Severity: Critical

Instance: "error parsing iptables output"

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeErrorParsingIptablesOutputNotify

Recovery:

Contact the *Customer Care Center* for assistance.

5011 - System or platform error prohibiting operation

Alarm Type: IPFE

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

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

Severity: Critical

Instance:

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

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

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeSystemErrorNotify

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

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

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

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

4. Click **OK** to continue.
5. If the alarm still does not clear, check the Ethernet devices and CPUs.

2. Contact the *Customer Care Center* for assistance.

5012 - Signaling interface heartbeat timeout

Alarm Type: IPFE

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

Severity: Critical

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

HA Score: Degraded

Auto Clear Seconds N/A

OID: ipfeIpfeSignalingInterfaceNotify

Recovery:

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

5013 - Throttling traffic

Alarm Type: IPFE

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

Severity: Critical

Instance: The number of packets that have been throttled

HA Score: Degraded

Auto Clear Seconds N/A

OID: ipfeIpfeThrottlingTrafficNotify

Recovery:

1. Compare the setting for the **Global Packet Rate Limit** configuration found under **IPFE** > **Configuration** > **Options** with the system's performance specifications and determine if a higher setting is reasonable.

2. Review macro conditions that lead to high signal rate.
3. If the problem persists, contact the *Customer Care Center*.

5100 - Traffic overload

Alarm Type: IPFE

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

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

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: ipfeIpfeTrafficOverloadNotify

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

The product is in excess of its design parameters, and may exhibit traffic loss if an additional failure occurs. Consider expanding system to accommodate additional capacity. Contact the *Customer Care Center* for assistance.

OAM (10000-10999)

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

10000 - Incompatible database version

Alarm Type: DB

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

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: 300

OID: tekelecIncompatibleDatabaseVersionNotify

Recovery: Contact the *Customer Care Center*.

10001 - Database backup started

Event Type: DB

Description: The database backup has started.

Severity: Info

Instance: GUI

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupStartNotify

Recovery: No action required.

10002 - Database backup completed

Event Type: DB

Description: Backup completed

Severity: Info

Instance: GUI

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupCompleteNotify

Recovery:

No action required.

10003 - Database backup failed

Event Type: DB

Description: The database backup has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupFailNotify

Recovery:

Contact the *Customer Care Center*.

10004 - Database restoration started

Event Type: DB

Description: The database restoration has started.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreStartNotify

Recovery:

No action required.

10005 - Database restoration completed

Event Type: DB

Description: The database restoration is completed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds:

OID: tekelecRestoreCompleteNotify

Recovery:

No action required.

10006 - Database restoration failed

Event Type: DB

Description: The database restoration has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreFailNotify

Recovery:

Contact the *Customer Care Center*.

10008 - Database provisioning manually disabled

Alarm Type: 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: tekelecProvisioningManuallyDisabled

Recovery:

No action required.

10009 - Config and Prov db not yet synchronized

Alarm Type: REPL

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

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: oAGTCfgProvDbNoSync

Recovery:

1. Monitor the replication status using the Status & Manage > Replication GUI page.
2. If alarm persists for more than one hour, contact the *Customer Care Center*.

10010 - Stateful db from mate not yet synchronized

Alarm Type: 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: oAGTStDbNoSync

Recovery:

If alarm persists for more than 30 seconds, contact the *Customer Care Center*.

10011 - Cannot monitor table

Alarm Type: 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: oAGTCantMonitorTable

Recovery:

Contact the *Customer Care Center*.

10012 - Table change responder failed

Alarm Type: 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: oAGTResponderFailed

Recovery:

Contact the *Customer Care Center*.

10013 - Application restart in progress

Alarm Type: 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: oAGTApplSWDisabled

Recovery:

If duration of alarm is greater than two seconds, contact the *Customer Care Center*.

10020 - Backup failure

Alarm Type: DB

Description: Database backup failed.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: apwBackupFailure

Recovery:

Alarm will clear if a backup (Automated or Manual) of the same group data is successful. Contact the *Customer Care Center* if failures persist.

10050 - Resource Audit Failure

Alarm Type: AUD

Description: Database backup failed.

Severity: Minor

Instance:

HA Score: Normal

Auto Clear Seconds: 0

OID: tekelecResourceAuditFailure

Recovery:

10051 - Route Deployment Failed

Alarm Type: 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: tekelecRouteDeploymentFailed

Recovery:

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

10052 - Route discovery failed

Alarm Type: AUD

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: tekelecRouteDiscoveryFailed

Recovery:

If the problem persists, contact the *Customer Care Center*.

10053 - Route deployment failed - no available device

Alarm Type: 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: tekelecNoRouteDevice

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 Type: 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: tekelecDeviceDeploymentFailed

Recovery:

Edit or delete the device.

10055 - Device discovery failed

Alarm Type: AUD

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: tekelecDeviceDiscoveryFailed

Recovery:

If the problem persists, contact the *Customer Care Center*.

10074 - Standby server degraded while mate server stabilizes

Alarm Type: 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: hASbyRecoveryInProgress

Recovery:

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

10075 - Application processes have been manually stopped

Alarm Type: HA

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

Severity: Minor

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: haMtceStopApplications

Recovery:

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

Once successfully restarted the alarm will clear.

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

Event Type: HA

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

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: failureRecoveryWithoutAppRestart

Recovery:

Contact the *Customer Care Center*.

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: tekelecLogExportStart

Recovery:

No action required.

10101 - Log export successful

Event Type: LOG

Description: The log files export operation completed successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecLogExportSuccess

Recovery:

No action required.

10102 - Log export failed

Event Type: LOG

Description: The log files export operation failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecLogExportFailed

Recovery:

1. Verify the export request and try the export again.
2. If the problem persists, contact the *Customer Care Center*.

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: tekelecLogExportNotRun

Recovery:

Restart export operation after existing export completes.

10104 - Log export file transfer failed

Event Type: LOG

Description: The performance data export remote copy operation failed.

Severity: Info

Instance: <Task ID>

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

HA Score: Normal

Throttle Seconds: 1

OID: tekelecExportXferFailed

Recovery:

Contact the *Customer Care Center* 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: tekelecLogExportCancelledUser

Recovery:

Contact the *Customer Care Center* 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: tekelecLogExportCancelledDuplicate

Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. If the problem persists, contact the *Customer Care Center* 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: tekelecLogExportCancelledDuplicate

Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.
2. If the problem persists, contact the *Customer Care Center* for assistance.

10108 - Duplicate scheduled log export task

Alarm Type: 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: tekelecLogExportDupSchedTask

Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. If the problem persists, contact the *Customer Care Center* for assistance.

10109 - Log export queue is full

Alarm Type: 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: tekelecLogExportQueueFull

Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure that the queue does not fill up.
2. If the problem persists, contact the *Customer Care Center* for assistance.

10151 - Login successful

Event Type: LOG

Description: The login operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecLoginSuccess

Recovery:

No action required.

10152 - Login failed

Event Type: LOG

Description: The login operation failed

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecLoginFailed

Recovery:

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

10153 - Logout successful

Event Type: LOG

Description: The logout operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecLogoutSuccess

Recovery:

No action required.

10154 - User Account Disabled

Alarm Group: AUTH

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: tekelecAccountDisabled

Recovery:

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

10155 - SAML Login Successful

Alarm Type: LOG

Description: SAML Login Successful

Severity: Info

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tekelecSamlLoginSuccess

Recovery:

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

10156 - SAML Login Failed

Alarm Type: LOG

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

Severity: Info

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tekelecSamlLoginFailed

Recovery:

1. Use correct username and password to log in.
2. For failed SSO login, verify SSO was properly configured. Collect logs and contact the *Customer Care Center* if the problem persists.

10200 - Remote database reinitialization in progress

Alarm Type: CFG

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

Severity: Minor

Instance: <hostname of remote server>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: apwSgDbReinit

Recovery:

1. Check to see that the remote server is configured.
2. Make sure the remote server is responding to network connections.
3. If this does not clear the alarm, delete this server from the server group.
4. If the problem persists, contact the *Customer Care Center*.

IDIH (11500-11549)

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

11500 - Tracing Suspended

Alarm Group: IDIH

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterTracingSuspendedAlarmNotify

Recovery:

No action required

11501 - Trace Throttling Active

Alarm Group: IDIH

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterTracingThrottledAlarmNotify

Recovery:

No action required

11502 - Troubleshooting Trace Started

Event Group: IDIH

Description: A troubleshooting trace instance was started.

Severity: Info

Instance: <TraceInstanceId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDIHTraceStartedNotify

Recovery:

No action required.

11503 - Troubleshooting Trace Stopped

Event Group: IDIH

Description: A troubleshooting trace instance was stopped.

Severity: Info

Instance: <TraceInstanceId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDIHTraceStoppedNotify

Recovery:

No action required

11504 - Invalid DIH IP Address

Alarm Group: IDIH

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

Severity: Minor

Instance: String of Configured DIH IP Address

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterTInvalidDihIpAddressAlarmNotify

Recovery:

No action required

Session Binding Repository, SBR (12000-12010)

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

12003 - SBR Congestion State

Alarm Type: SBRA

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

Table 10: Congestion Thresholds

Severity	Set Threshold	Clear Threshold	Shed Operations	Associated Measurements
Minor	60%	50%	Creates	*Sbr.TxShedCreates*

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

Severity: Minor, Major, Critical

Instance: Sbr.RxIngressMsgQueueMetric[subId], SBR

HA Score: Normal

Auto Clear Seconds: N/A

OID: SbrCongestionState

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

The SBR congestion status exceeds the alarm threshold. Additional capacity may be required to service the traffic load. Contact the *Customer Care Center* for assistance.

12007 - SBR Active Sess Binding Threshold

Alarm Type: SBRA

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

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

Severity: Minor, Major, Critical

Instance: Sbr.EvCurrentSessionMetric, SBR

HA Score: Normal

Auto Clear Seconds: N/A

OID: SbrActiveSessBindThreshold

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

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

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

2. Increase the **Maximum active session bindings** configuration if it is too low.
3. Click **Apply** to apply your changes.

   Your changes will go into affect immediately.

4. The SBR active session bindings count exceeds the threshold. Additional capacity may be required to service the traffic load. Contact the *Customer Care Center* for assistance.

12010 - SBR Proc Term

Alarm Type: SBRA

Description: The SBR application has terminated.

Severity: Critical

Instance: sbr

HA Score: Degraded

Auto Clear Seconds: 10

OID: SbrProcTerm

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

1. Check the status of the terminated SBR by navigating to the **Status & Manage > Server** page.
2. If the Process Manager cannot restart the process, contact the *Customer Care Center* for assistance.

Communication Agent, ComAgent (19800-19909)

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

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

19800 - Communication Agent Connection Down

Alarm Type: CAF

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFConnectionDownNotify

Recovery:

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. If the connection is manually disabled, then no further action is necessary.
5. Verify that the remote server is not under maintenance.
6. Verify that IP network connectivity exists between the two connection end-points.
7. Verify that the connection's local IP address and port number are configured on remote Node.
8. Verify that the Application Process using Communication Agent plug-in is running on both ends.
9. Verify that the connection's remote IP address and port correctly identify remote's listening port.
10. Contact the *Customer Care Center* for assistance.

19801 - Communication Agent Connection Locally Blocked

Alarm Type: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFConnLocalBlockedNotify

Recovery:

This alarm is cleared when:

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

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. If the expected set of connections is locally blocked, then no further action is necessary.
5. To remove a the local block condition for a connection, use the **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screen and click the 'Enable' action button for the desired connection.
6. Contact the *Customer Care Center* for assistance.

19802 - Communication Agent Connection Remotely Blocked

Alarm Type: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFConnRemoteBlockedNotify

Recovery:

This alarm is cleared when:

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

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. If the expected set of connections is locally blocked, then no further action is necessary.
5. To remove a the local block condition for a connection, use the **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screen and click the 'Enable' action button for the desired connection.
6. Contact the *Customer Care Center* for assistance.

19803 - Communication Agent stack event queue utilization

Alarm Type: CAF

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

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFQueueUtilNotify

Recovery:

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

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

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

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

   Contact the *Customer Care Center* for assistance.

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

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

   Contact the *Customer Care Center* for assistance.

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

Alarm Type: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 300 (5 min)

OID: CAFClientConnWaitNotify

Recovery:

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

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

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

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

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

8. Verify that the connection's local IP address and port number are configured on remote client MP.
9. Verify that the Application Process using Communication Agent plug-in is running on both ends.
10. Verify that the connection's remote IP address and port correctly identify remote's listening port.
11. Contact the *Customer Care Center* for assistance.

19805 - Communication Agent Failed To Align Connection

Alarm Type: CAF

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFConnAlignFailedNotify

Recovery:

1. If the connection administrative action is set to 'disable', the alarm is cleared. No further action is necessary.
2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
4. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
5. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

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

6. Contact the *Customer Care Center* for assistance.

19806 - Communication Agent CommMessage mempool utilization

Alarm Type: CAF

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

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

Severity: Critical, Major, Minor

Instance: <ComAgent Process Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFPoolResUtilNotify

Recovery:

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

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

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

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

   Contact the *Customer Care Center* for assistance.

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

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

   Contact the *Customer Care Center* for assistance.

19807 - Communication Agent User Data FIFO Queue utilization

Alarm Type: CAF

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

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFUserDataFIFOUtilNotify

Recovery:

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

   Contact the *Customer Care Center* for assistance.

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

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

   Contact the *Customer Care Center* for assistance.

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

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

   Contact the *Customer Care Center* for assistance.

19808 - Communication Agent Connection FIFO Queue utilization

Alarm Type: 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: CAFConnectionFIFOUtilNotify

Recovery:

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

   Contact the *Customer Care Center* for assistance.

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

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

Contact the *Customer Care Center* for assistance.

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

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

   Contact the *Customer Care Center* for assistance.

19810 - Communication Agent Egress Message Discarded

Event Type: CAF

Description: Communication Agent Egress Message Discarded.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventEgressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

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

2. If it's a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, It's an indication that the Communication Agent Process may be experiencing problems.
4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
5. Contact the *Customer Care Center* for assistance.

19811 - Communication Agent Ingress Message Discarded

Event Type: CAF

Description: Communication Agent Ingress Message Discarded.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventIngressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

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

2. If it's a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, it is an indication that the Communication Agent Process may be experiencing problems.
4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
5. Contact the *Customer Care Center* for assistance.

19814 - Communication Agent Peer has not responded to heartbeat

Event Type: CAF

Description: Communication Agent Peer has not responded to heartbeat.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventHeartbeatMissedNotify

Recovery:

1. Check the configuration of managed objects and resolve any configuration issues with the Managed Object or hosting nodes.

   This message may be due to network condition or latency or due to setup issues.

2. If the event is raised due to software condition, It's an indication that the Communication Agent Process may be experiencing problems.
3. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
4. Contact the *Customer Care Center* for assistance.

19816 - Communication Agent Connection State Changed

Event Type: CAF

Description: Communication Agent Connection State Changed.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventConnectionStateChangeNotify

Recovery:

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

   This Event is a log of connection state change.

2. Contact the *Customer Care Center* for assistance.

19817 - Communication Agent DB Responder detected a change in configurable control option parameter

Event Type: CAF

Description: Communication Agent DB Responder detected a change in configurable control option parameter.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtConfigParamChangeNotify

Recovery:

This event is an indication that Communication Agent detected a control parameter change. The change will be applied to applicable software component. If the change is applied on the GUI, the appropriate GUI action is logged in security logs. If the action is not performed from GUI and the control parameter is changed, this event indicates the executed change.

1. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
2. Use **Main Menu** > **Security Log** and examine the alarm log.
3. If the event shows up in **Main Menu** > **Alarms & Events**, without the corresponding GUI security-log in **Main Menu** > **Security Log**. Contact the *Customer Care Center* for assistance.

19818 - Communication Agent DataEvent Mempool utilization

Event Type: CAF

Description: The percent utilization of the Communication Agent DataEvent Mempool is approaching defined threshold capacity.

Severity: Minor, Major, Critical

Instance: <ComAgent Process>

HA Score: Normal

Throttle Seconds: 86400

OID: cAFDataEvPoolResUtilNotify

Recovery:

If the problem persists, contact the *Customer Care Center*.

19820 - Communication Agent Routed Service Unavailable

Alarm Type: CAF

Description: This alarm indicates that all connections of all connection groups associated with a Routed Service are unavailable. This generally occurs when far-end servers have been removed from service

by maintenance actions. This can also occur if all of the Routed Service's connections have been either disabled or blocked.

Severity: Major

Instance: <RoutedServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFRSUnavailNotify

Recovery:

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

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. Contact the *Customer Care Center* for assistance.

19821 - Communication Agent Routed Service Degraded

Alarm Type: CAF

Description: This alarm indicates that some, but not all, connections are unavailable in the connection group being used by a Communication Agent Routed Service to route messages. The result is that the server that posted this alarm is not load-balancing traffic across all of the connections configured in the connection group.

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFRSDegradedNotify

Recovery:

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

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. Contact the *Customer Care Center* for assistance.

19822 - Communication Agent Routed Service Congested

Alarm Type: CAF

Description: This alarm indicates that a routed service is load-balancing traffic across all connections in a connection group, but all of the connections are experiencing congestion. Messages may be discarded due to congestion.

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFRSCongestedNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the the are congested and the degree to which they are congested.
3. Check the far-end of the congested connections in order to further isolate the cause of congestion.

   If the far-end servers are overloaded, then it is possible that the system is being presented a load that exceeds its engineered capacity. If this is the case, then either the load must be reduced, or additional capacity must be added.

4. Contact the *Customer Care Center* for assistance.

19823 - Communication Agent Routed Service Using Low-Priority Connection Group

Alarm Type: CAF

Description: Communication Agent routed service is routing traffic using a connection group that has a lower-priority than another connection group.

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFRSUsingLowPriConnGrpNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the the reasons why connections are unavailable.

3. Use **Main Menu** > **Status & Manage** > **Server** to confirm that the far-end servers have an application state of enabled, and that their subsystems are operating normally.

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. Contact the *Customer Care Center* for assistance.

19824 - Communication Agent Pending Transaction Utilization

Alarm Type: CAF

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

Severity: Minor, Major, Critical

Instance: n/a (ComAgent process)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFTransUtilNotify

Recovery:

1. Use **Main Menu** > **Status & Control** > **Server Status** to view MP server status.
2. Remote server is slow in responding to outstanding transaction with correlation resource in-use. The mis-configuration of ComAgent Server/Client routing may result in too much traffic being distributed to affected connection for MP.
3. There may be an insufficient number of Server Application MPs configured to handle the internal traffic load. If server application MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. Use **Main Menu** > **Alarm & Events** and examine the alarm log.

   The system may be experiencing network problems.

   The Communication Agent Process may be experiencing problems.

5. Contact the *Customer Care Center* for assistance.

19825 - Communication Agent Transaction Failure Rate

Alarm Type: CAF

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

Severity: Minor, Major, Critical

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFTransFailRateNotify

Recovery:

1. Use **Main Menu** > **Status & Control** > **Server Status** to view MP server status.
2. Remote server is slow in responding to outstanding transaction with correlation resource in-use. The mis-configuration of ComAgent Server/Client routing may result in too much traffic being distributed to affected connection for MP.
3. There may be an insufficient number of Server Application MPs configured to handle the internal traffic load. If server application MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. Use **Main Menu** > **Alarm & Events** and examine the alarm log.

   The system may be experiencing network problems.

   The Communication Agent Process may be experiencing problems.

5. Contact the *Customer Care Center* for assistance.

19826 - Communication Agent Connection Congested

Alarm Type: CAF

Description: This alarm indicates that Communication Agent is experiencing congestion in communication between two servers, and this can be caused by a server becoming overloaded or by network problems between two servers.

Severity: Major

Instance:N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFConnCongestedNotify

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. If the Remote MP Overload Level (OL) > 0 then determine why the remote server is congested.
   a) Verify that the remote server is not under maintenance.
   b) Examine the remote's CPU utilization.
   c) Examine the remote's current alarms.
5. If the local server's Transport Congestion Level (TCL) > 0 then determine why the connection is not handling the load.
   a) The remote may be overload by traffic from other MPs.
   b) The local server may be trying to send too much traffic to the remote.
   c) The IP connectivity may be impaired.

6. Contact the *Customer Care Center* for assistance.

19830 - Communication Agent Service Registration State Change

Event Type: CAF

Description: Communication Agent Service Registration State Change.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtSvcRegChangedNotify

Recovery:

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

19831 - Communication Agent Service Operational State Changed

Event Type: CAF

Description: Communication Agent Service Operational State Changed.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtSvcOpStateChangedNotify

Recovery:

1. This event indicates that a Communication Agent service changed operational state, and typically results from maintenance actions.

   A service can also change state due to server overload.

2. If the state change is unexpected, then Contact the *Customer Care Center* for assistance.

19832 - Communication Agent Reliable Transaction Failed

Event Type: CAF

Description: Failed transaction between servers result from normal maintenance actions, overload conditions, software failures, or equipment failures.

Severity: Info

Instance: <ServiceName>, <RemoteIP> |< null>

- If serviceID is InvalidServiceID, then <ServiceName> is “EventTransfer”.
- If <ServiceName> is “EventTransfer”, then include <RemoteIP>.
- If serviceID is unknown, then <ServiceName> is null.

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventComAgtTransFailedNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if the local server is unable to communicate with another server or if servers have become overloaded.
2. Check the server’s KPIs and the **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to trouble-shoot the cause of server overload.
3. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **HA Status** that corresponds to the ServiceID in the event instance to trouble-shoot the operation of the service.
4. If the event cannot be explained by maintenance actions, then Contact the *Customer Care Center* for assistance.

19833 - Communication Agent Service Egress Message Discarded

Event Type: CAF

Description: Communication Agent Service Egress Message Discarded.

Severity: Info

Instance: <ServiceName>, <RemoteIP> |< null>

- If serviceID is unknown, then <ServiceName> is null.

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventRoutingFailedNotify

Recovery:

1. View the Event AddlInfo column.

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

2. If it’s a persistent condition with the status of one of the Communication Agent Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, It’s an indication that the Communication Agent Process may be experiencing problems.
4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
5. Contact the *Customer Care Center* for assistance.

19842 - Communication Agent Resource-Provider Registered

Event Type: CAF

Description: Communication Agent Resource-Provider Registered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceProviderRegisteredNotify

Recovery:

No action required.

19843 - Communication Agent Resource-Provider Resource State Changed

Event Type: CAF

Description: Communication Agent Resource-Provider Resource State Changed.

Severity: Info

Instance: <ProviderServerName>: <ResourceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventResourceStateChangeNotify

Recovery:

No action required.

19844 - Communication Agent Resource-Provider Stale Status Received

Event Type: CAF

Description: Communication Agent Resource-Provider Stale Status Received.

Severity: Info

Instance: <ProviderServerName>: <ResourceName>

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventStaleHBPacketNotify

Recovery:

If this event is occurring frequently then check the ComAgent maintenance screens for other anomalies and to troubleshoot further.

19845 - Communication Agent Resource-Provider Deregistered

Event Type: CAF

Description: Communication Agent Resource-Provider Deregistered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceProviderDeRegisteredNotify

Recovery:

No action required.

19846 - Communication Agent Resource Degraded

Alarm Type: 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: CAFResourceDegradedNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which sub-resources are unavailable or degraded for the server that asserted the alarm.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if connections have failed or have congested.
3. Contact the *Customer Care Center* for assistance.

19847 - Communication Agent Resource Unavailable

Alarm Type: CAF

Description: Communication Agent Resource Unavailable. A local application needs to use a ComAgent resource, but the resource is unavailable. The resource can be unavailable if the local server has no ComAgent connections to servers providing the resource or no servers host active instances of the resource's sub-resources.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: CAFResourceUnavailNotify

Recovery: Check the Communication Agent Connection Status maintenance screen

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to verify that the local server is connected to the expected servers.

   If the local server reports unavailable connections, then take actions to troubleshoot the cause of the connection failures.

2. If the ComAgent connections are InService, use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which servers are providing the resource.

   If no servers are providing the resource, then the most likely reason is that maintenance actions have been taken that have removed from service the application that provides the concerned resource.

3. Contact the *Customer Care Center* for assistance.

19848 - Communication Agent Resource Error

Alarm Type: CAF

Description: Communication Agent Resource Error. Two sets of servers are using incompatible configurations for a ComAgent resource.

Severity: Minor

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 50

OID: CAFResourceErrorNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which sets of servers are incompatible.

   Check the incompatible servers to verify that they are operating normally and are running the expected versions of software.

2. Contact the *Customer Care Center* for assistance.

19850 - Communication Agent Resource-User Registered

Event Type: CAF

Description: Communication Agent Resource-User Registered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceUserRegisteredNotify

Recovery:

No action required.

19851 - Communication Agent Resource-User Deregistered

Event Type: CAF

Description: Communication Agent Resource-User Deregistered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceUserDeRegisteredNotify

Recovery:

No action required.

19852 - Communication Agent Resource Routing State Changed

Event Type: CAF

Description: Communication Agent Resource Routing State Changed.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventResourceRoutingStateNotify

Recovery:

No action required.

19853 - Communication Agent Resource Egress Message Discarded

Event Type: CAF

Description: Communication Agent Resource Egress Message Discarded.

Severity: Info

Instance: <ResourceName>: <SubResourceID>

Note: If the resource is unknown, then <ResourceName> is the ResourceID converted to text. The <SubResourceID> is an integer converted to text, regardless of whether it is known or unknown.

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventHaEgressMessageDiscarded

Recovery:

1. Message is being discarded due to one of the reasons specified in Event AddlInfo.

   If the condition is persistent with the status of one of the ComAgent Configuration Managed Objects there is an underlying issue with the Managed Object.

2. Use **Main Menu** > **Alarms & Events** and examine the alarm log for ComAgent Process problems.
3. Contact the *Customer Care Center* for assistance.

19854 - Communication Agent Resource-Provider Tracking Table Audit Results

Event Type: CAF

Description: Communication Agent Resource-Provider Tracking Table Audit Results. This event is generated when a Resource Provider Tracking Table (RPTT) entry with Status equal to Auditing is replaced with a new status (null, Active, Standby, Spare, OOS, etc) and there are no other RPTT entries, for this specific Resource/SR, with Status equal to Auditing.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventHaRPTTAuditResultNotify

Recovery:

No action required.

19855 - Communication Agent Resource Has Multiple Actives

Alarm Type: 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: CAFResourceMultActiveNotify

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which Resource Provider servers are announcing 'Active' status for the Resource.
2. Investigate possible IP network isolation between these Resource Provider servers.
3. Contact the *Customer Care Center* for assistance.

19856 - Communication Agent Service Provider Registration State Changed

Event Type: CAF

Description: The Communication Agent Service Provider Registration State has changed.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventSvcProvRegStateChangedNotify

Recovery:

1. This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.
2. Contact the *Customer Care Center* for further assistance.

19857 - Communication Agent Service Provider Operational State Changed

Event Type: CAF

Description: The Communication Agent Service Provider Operational State has Changed

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventSvcProvOpStateChangedNotify

Recovery:

1. This event indicates that a ComAgent service provider changed operational state, and typically results from maintenance actions. A service can also change state due to overload.
2. If the state change is unexpected, contact the *Customer Care Center*.

19860 - Communication Agent Configuration Daemon Table Monitoring Failure

Alarm Type: 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: CAFDaemonTableMonitorFailureNotify

Recovery:

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. If conditions do not permit a forced failover of the active NOAM, then contact the *Customer Care Center* for assistance.
4. If conditions permit, then initiate a failover of active NOAM.

   This causes the Communication Agent Configuration Daemon to exit on the originally-active NOAM and to start on the newly-active NOAM.

5. After NOAM failover completes, verify that the alarm has cleared.
6. If the alarm has not cleared, then Contact the *Customer Care Center* for assistance.

19861 - Communication Agent Configuration Daemon Script Failure

Alarm Type: 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: CAFDaemonScriptFailureNotify

Recovery:

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

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this server.
3. If conditions do not permit a forced failover of the active NOAM, then contact the *Customer Care Center* for assistance.
4. If conditions permit, then initiate a failover of active NOAM.

   This causes the Communication Agent Configuration Daemon to exit on the originally-active NOAM and to start on the newly-active NOAM.
5. After NOAM failover completes, verify that the alarm has cleared.
6. If the alarm has not cleared, then Contact the *Customer Care Center* for assistance.

19862 - Communication Agent Ingress Stack Event Rate

Alarm Group: CAF

Description: The Communication Agent Ingress Stack Event Rate is approaching its defined threshold capacity.

Severity:

- Minor - if exceeding 100K on Gen8 hardware, 75k on other hardware
- Major - if exceeding 110K on Gen8 hardware, 80k on other hardware
- Critical - if exceeding 120K on Gen8 hardware, 84k on other hardware

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds 0 (zero)

OID: CAFIngresRateNotify

Recovery:

1. This alarm indicates that a server is overrunning its defined processing capacity. If any of the defined threshold onset levels are exceeded, Communication Agent will discard comparatively low priority messages. Check the configuration, routing, and deployment mode capacity.
2. Contact the *Customer Care Center* for further assistance.

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group: CAF

Description: The maximum number of connections per connection group limit has been reached.

Severity: Info

Instance: <Connection group name>

HA Score: Normal

Throttle Seconds: 86400

OID: cAFComAgentMaxConnsInGrpNotify

Recovery:

1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.
2. Contact the *Customer Care Center* for further assistance.

19864 - ComAgent Successfully Set Host Server Hardware Profile

Event Group: CAF

Description: ComAgent successfully set the host server hardware profile.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventSuccessSetHostServerHWProfileNotify

Recovery:

1. This event indicates that all TPS controlling parameter values are successfully set for the host server hardware profile.
2. If needed, contact the *Customer Care Center*.

19865 - ComAgent Failed to Set Host Server Hardware Profile

Event Group: CAF

Description: ComAgent failed to set the host server hardware profile.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventFailToSetHostServerHWProfileNotify

Recovery:

1. This event indicates that there is a failure in applying default hardware settings for ComAgent TPS controlling parameters. When default settings also fail to apply, then the factory values will be used for the TPS controlling parameters.
2. If needed, contact the *Customer Care Center*.

19900 - Process CPU Utilization

Alarm Type: STK

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

Severity: Critical, Major, Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcProcessCpuUtilizationNotify

Recovery:

1. Use **Main Menu** > **Status & Control** > **KPIs** to monitor the ingress traffic rate of each MP.
   - The mis-configuration of Server/Client routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
   - There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the traffic load to the server site is exceeding its capacity.
2. Use **Main Menu** > **Alarms & Events** to examine the alarm log.

   Contact the *Customer Care Center* for assistance.

19901 - CFG-DB Validation Error

Alarm Type: 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: STKcfgDbValidationErrorNotify

Recovery:

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

Contact the *Customer Care Center* for assistance.

19902 - CFG-DB Update Failure

Alarm Type: 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: STKcfgDbUpdateFailureNotify

Recovery:

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

Contact the *Customer Care Center* for assistance.

19903 - CFG-DB post-update Error

Alarm Type: 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: STKcfgDbPostUpdateErrorNotify

Recovery:

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

Contact the *Customer Care Center* for assistance.

19904 - CFG-DB post-update Failure

Alarm Type: 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: STKcfgDbPostFailureNotify

Recovery:

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

Contact the *Customer Care Center* for assistance.

19905 - Measurement Initialization Failure

Alarm Type: STK

Description: A measurement object failed to initialize.

Severity: Critical

Instance: <measTagName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: STKmeasurementInitializationFailureNotify

Recovery:

Measurement subsystem initialization has failed for the specified measurement.

Contact the *Customer Care Center* for assistance.

Diameter Signaling Router (DSR) Diagnostics (19910-19999)

This section provides information and recovery procedures for DSR alarms and events, ranging from 19910-19999, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

19910 - Message Discarded at Test Connection

Event Type: DIAG

Description: Normal traffic is being discarded because it is routed to an egress Test Connection. An egress Test Connection is given a normal message to be transmitted.

Severity: Major

Instance: <Connection name>

HA Score: Normal

Throttle Seconds: 86400

OID: dbcNormalMessageDiscardedNotify

Recovery:

1. Update routing rules to exclude Test connections from being used for routing.

   Normal traffic should be received and sent on non-test connections.

2. Change the hostname of the peer connected to the test connection.

   The hostname of the peer connected to the test connection may be the destination host for the incoming normal traffic.

19911 - Test message discarded

Event Type: DIAG

Description: Test message is given to a non-test connection to be transmitted.

Severity: Info

Instance: <Connection name>

HA Score: Normal

Throttle Seconds: 5

OID: dbcDiagnosticMessageDiscardNotify

Recovery:

Update routing rules to exclude Test messages from being routed to non-test connection.

Test messages should be received and sent only on test connections.

Diameter Alarms and Events (22000-22350, 22900-22999)

22001 - Message Decoding Failure

Event Type: DIAM

Description: A message received from a peer was rejected because of a decoding failure. Decoding failures can include missing mandatory parameters. A Diameter message was received either without the mandatory Destination-Realm AVP or, while parsing the message, the message content was inconsistent with the Message Length in the message header.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterIngressMsgRejectedDecodingFailureNotify

Recovery:

These protocol violations are caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node (identified by the Peer Name) and cannot be fixed using the application.

22002 - Peer Routing Rules with Same Priority

Event Type: DIAM

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

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterPeerRoutingTableRulesSamePriorityNotify

Recovery:

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

22003 - Application ID Mismatch with Peer

Event Type: DIAM

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

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterApplicationIdMismatchWithPeerNotify

Recovery:

1. The system's peer routing table may be using a Route List containing a peer which does not support the Application ID or the list of Application IDs supported by the peer on each connection may not be the same. The list of Application IDs that the peer supports on each connection can be viewed as follows:
   a) Navigate to the GUI page: **Diameter > Maintenance > Connections**
   b) Locate the relevant Peer Node and check the supported Application IDs.
2. If Application IDs are not the same for each connection (but should be) the Application ID for any connection can be refreshed by:
   a) Navigate to the GUI page: **Diameter > Maintenance > Connections**

b) Locate the relevant **Connection**
c) Disable the **Connection**
d) Enable the **Connection**

3. The Diameter Node which originated the message (identified by the Origin-Host AVP) could be configured incorrectly and the application is trying to address a node which doesn't support the Application ID. This cannot be fixed using this application.
4. If the problem persists, contact the *Customer Care Center*.

22004 - Maximum pending transactions allowed exceeded

Event Type: DIAM

Description: Routing attempted to select an egress transport connection to forward a message but the maximum number of allowed pending transactions queued on the connection has been reached.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterMaxPendingTxnsPerConnExceededNotify

Recovery:

The maximum number of pending transactions for each connection is set to a system-wide default value. If this event is occurring frequently enough for a particular connection then the maximum value may need to be increased. Contact the *Customer Care Center* 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: eagleXgDiameterForwardingNoPrtRuleNotify

Recovery:

1. Either the message was incorrectly routed to this node or additional Peer Routing Rules need to be added. Existing Peer Routing Rules can be viewed and updated using **Diameter > Configuration > Peer Routing Rules** page.
2. If the problem persists, contact the *Customer Care Center*.

22006 - Forwarding Loop Detected

Event Type: DIAM

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

Severity: Info

Instance: <PeerName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterForwardingLoopDetectedNotify

Recovery:

1. An ingress Request message was rejected because message looping was detected. In general, the forwarding node should not send a message to a peer which has already processed the message (it should examine the Route-Record AVPs prior to message forwarding). If this type of error is occurring frequently, then the forwarding node is most likely incorrectly routing the message and the issue cannot be fixed using this application.
2. If Path Topology Hiding is activated and Protected Network Node's Route-Records are obscured with PseudoNodeFQDN, then inter-network ingress message loop detection could reject the message if same Request message is routed back to DEA. If this type of error is occurring, then the forwarding node is most likely mis-routing the message back to DEA.
3. If the problem persists, contact the *Customer Care Center*.

22007 - Inconsistent Application ID Lists from a Peer

Event Type: DIAM

Description: The list of Application IDs supported by a peer during the Diameter Capabilities Exchange procedure on a particular transport connection is not identical to one of the list of Application IDs received from the peer over a different available transport connection to that peer.

Severity: Info

Instance: <PeerName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSupportedAppIdsInconsistentNotify

Recovery:

1. A peer with multiple transport connections has established a connection and provided a list of supported Application IDs which does match a previously established connection. This could prevent Request messages from being routed uniformly over the peer's transport connections because the decision to route a message containing an Application ID is based upon the list of Application IDs supported on each transport connection. The list of Application IDs that the peer supports on each connection can be viewed as follows:
   a) Navigate to **Diameter > Maintenance > Connections**.

b) Locate the relevant Peer Node and check the supported Application IDs.

2. If Application IDs are not the same for each connection (but should be) the Application ID for any connection can be refreshed by:
   a) Navigate to **Diameter > Maintenance > Connections**.
   b) Locate the relevant Connection.
   c) Disable the Connection.
   d) Enable the Connection.
3. If the problem persists, contact the *Customer Care Center*.

22008 - Orphan Answer Response Received

Event Type: DIAM

Description: An Answer response was received for which no pending request transaction existed, resulting in the Answer message being discarded. When a Request message is forwarded the system saves a pending transaction, which contains the routing information for the Answer response. The pending transaction is abandoned if an Answer response is not received in a timely fashion.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterOrphanAnswerResponseReceivedNotify

Recovery:

If this event is occurring frequently, the transaction timers may be set too low. The timer values can be viewed and/or modified using the **Diameter > Configuration > System Options** page.

22009 - Application Routing Rules with Same Priority

Event Type: DIAM

Description: An application routing table search with a received Request message found more than one highest priority application routing rule match. At least two application routing rules with the same priority matched an ingress Request message. The system selected the first application routing rule found.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterApplicationRoutingTableRulesSamePriorityNotify

Recovery:

1. It is recommended that application routing rules be unique for the same type of messages to avoid unexpected routing results. Peer routing rule priorities can be modified using **Diameter > Configuration > Application Routing Rules** page.
2. If the problem persists, contact the *Customer Care Center*.

22010 - Specified DAS Route List not provisioned

Event Type: DIAM

Description: The DAS Route List specified by the message copy trigger point is not provisioned.

Severity: Info

Instance: <RouteListId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSpecifiedDasRouteListNotProvisionedNotify

Recovery:

1. Provisioning is incorrect/misconfigured. Verify provisioning and provision/correct provisioning.
2. If this problem persists, contact the *Customer Care Center* for assistance.

22012 - Specified MCCS not provisioned

Event Type: DIAM

Description: The Message copy CfgSet attached to the original message by the trigger point is not provisioned

Severity: Info

Instance: <MCCS>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSpecifiedMCCSNotProvisionedNotify

Recovery:

1. Verify the configured value of MCCS with the trigger point.
2. Verify the Message Copy CfgSet (MCCS) provisioning is properly configured.
3. If the problem persists, contact the *Customer Care Center*.

22014 - No DAS Route List specified

Alarm Type: DIAM

Description: No valid DAS Route List was specified in the Message Copy Config Set.

Severity: Info

Instance: <RouteListId>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterNoDasRouteListSpecifiedNotify

Recovery:

Contact the *Customer Care Center* 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 the *Customer Care Center*.

22016 - Peer Node Alarm Aggregation Threshold

Alarm Type: DIAM

Description: This alarm occurs when there are a 'Critical' number of Peer Node alarms for a single Network Element.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPeerNodeUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Peer Nodes** to monitor Peer status.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peer is not under maintenance.
5. Contact the *Customer Care Center* for assistance.

22017 - Route List Alarm Aggregation Threshold

Alarm Type: DIAM

Description: This alarm occurs when there are a 'Critical' number of Route List alarms for the Network Element.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Route Lists** to monitor Route List status.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List are not under maintenance.
5. Contact the *Customer Care Center* for assistance.

22018 - Maintenance Leader HA Notification to go Active

Alarm Type: DIAM

Description: This alarm occurs when a DA-MP has received a notification from HA that the Maintenance Leader resource should transition to the Active role.

Severity: Info

Instance: <MP Node ID>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterDaMpLeaderGoActiveNotificationNotify

Recovery:

No action necessary.

22019 - Maintenance Leader HA Notification to go OOS

Alarm Type: DIAM

Description: This alarm occurs when a DA-MP has received a notification from HA that the Maintenance Leader resource should transition to the OOS role.

Instance: <MP Node ID>

Severity: Info

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterDaMpLeaderGoOOSNotificationNotify

Recovery:

No action necessary.

22021 - Debug Routing Info AVP Enabled

Event Type: DIAM

Description: Debug Routing Info AVP is enabled.

Severity: Minor

Instance: None

HA Score: Normal

Throttle Seconds: 86400

OID: eagleXgDiameterDebugRoutingInfoAvpEnabledNotify

Recovery:

1. Change the IncludeRoutingInfoAvp parameter to *no* in the DpiOption table on the NO for a 2-tier system or on the SO for a 3-tier system.
2. If the problem persists, contact the *Customer Care Center*.

22051 - Peer Unavailable

Alarm Type: DIAM

Description: Unable to access the Diameter Peer because all of the transport connections are Down.

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPeerUnavailableNotify

Recovery:

1. Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peer is not under maintenance.
5. If the problem persists, contact the *Customer Care Center*.

22052 - Peer Degraded

Alarm Type: DIAM

Description: The peer has some available connections, but less than its minimum connection capacity. Continued routing to this peer may cause congestion or other overload conditions.

Severity: Major

Instance: <PeerName> (of the Peer which is degraded)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPeerDegradedNotify

Recovery:

1. Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peer is not under maintenance.
5. If the problem persists, contact the *Customer Care Center*.

22053 - Route List Unavailable

Alarm Type: DIAM

Description: The Route List is Unavailable. A Route List becomes Unavailable when all of its peers become Unavailable and a Peer becomes Unavailable when all of its transport connections become Unavailable.

If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.

Severity: Critical

Instance: <RouteListName> (of the Route List which failed)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListUnavailableNotify

Recovery:

1. Route List status can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List not under maintenance.
5. If the problem persists, contact the *Customer Care Center*.

22054 - Route List Degraded

Alarm Type: DIAM

Description: The Route List's Operational Status has changed to Degraded because the capacity of the Route List's Active Route Group has dropped below the Route List's configured minimum capacity. There are two potential causes:

1. One or more of the Route List's peers become Unavailable. A Peer becomes Unavailable when all of its transport connections become Unavailable. If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.
2. The Route Groups within the Route List may not have been configured with sufficient capacity to meet the Route List's configured minimum capacity.

Severity: Major

Instance: <RouteListName> (of the Route List which is degraded)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRouteListDegradedNotify

Recovery:

1. Route List status and configured minimum capacity can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List not under maintenance.
5. If the problem persists, contact the *Customer Care Center*.

22055 - Non-Preferred Route Group in Use

Alarm Type: DIAM

Description: The application has started to utilize a Route Group other than the highest priority Route Group to route Request messages for a Route List because the highest priority Route Group specified for that Route List has either become Unavailable or its capacity has dropped below the minimum capacity configured for the Route List while a lower priority Route Group has more capacity.

The preferred Route Group (i.e., with highest priority) is demoted from the Active Route Group to a Standby Route Group when a peer failure occurs causing the Route Group's Operational Status to change to Unavailable or Degraded. A Route Group becomes Degraded when its capacity has dropped

below Route List's configured minimum capacity. A Route Group becomes Unavailable when all of its peers have an Operational Status of Unavailable or Degraded.

A Peer becomes Unavailable when all of its transport connections become Unavailable. If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.

Severity: Minor

Instance: <RouteListName> (of the concerned Route List)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterNonpreferredRouteGroupInUseNotify

Recovery:

1. Route List status and configured minimum capacity can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, contact the *Customer Care Center*.

22057 - Egress Throttle Group Rate Limit Degraded

Alarm Type: DIAM

Description: The ETG Rate Limit has exceeded the defined threshold

Severity: Major

Instance: <ETGName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgRateLimitDegradedNotify

Recovery:

1. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Main Menu** > **Diameter** > **Maintenance** > **Connections** to determine if the sending Peers/Connections are offering too much traffic.
3. If the problem persists, contact the *Customer Care Center*.

22058 - Egress Throttle Group Pending Transaction Limit Degraded

Alarm Type: DIAM

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

Severity: Major

Instance: <ETGName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgPendingTransLimitDegradedNotify

Recovery:

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

22059 - Egress Throttle Group Message Rate Congestion Level changed

Event Group: DIAM

Description: The Egress Throttle Group Message rate Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity: N/A

Instance: <ETGName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterEtgRateCongestionNotify

Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and/or **Main Menu** > **Diameter** > **Maintenance** > **Connections**
3. Typically all routes to a server should be in an ETG. However, if that is not the case, alternate routes may be out of service and could cause overloading of traffic towards connections contained in this ETG. Evaluate traffic distribution to Server connections and see if any alternate routes to Server are unavailable causing overloading of traffic on an ETG.
4. Contact the *Customer Care Center* for assistance.

22060 - Egress Throttle Group Pending Transaction Limit Congestion Level changed

Event Group: DIAM

Description: The Egress Throttle Group Pending Transaction Limit Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity: N/A

Instance: <ETGName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterEtgPendingTransCongestionNotify

Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Main Menu** > **Diameter** > **Configuration** > **Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Main Menu** > **Diameter** > **Maintenance** > **Egress Throttle Groups** and/or **Main Menu** > **Diameter** > **Maintenance** > **Connections**
3. Typically all routes to a server should be in a ETG, however if that is not the case, then those routes becoming out of service could cause overloading of traffic towards connections contained in this ETG. Evaluate traffic distribution to Server connections and see if any alternate routes to Server are unavailable causing overloading of traffic on an ETG.
4. The receiving Peers or Connections in the ETG are not responding with Answers in a timely manner. Check to see if they are busy or overloaded.
5. If the problem persists, contact the *Customer Care Center* for assistance.

22061 - Egress Throttle Group Monitoring stopped

Alarm Type: DIAM

Description: ETG Rate and Pending Transaction Monitoring is stopped on all configured ETGs

Severity: Minor

Instance: <DA-MP Hostname>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterEtgMonitoringStoppedNotify

Recovery:

1. Verify that ComAgent links setup between DA-MPs have not gone OOS causing SMS Service to not receive Responses from DA-MP Leader under **Main Menu** > **Communication Agent** > **Maintenance**.
2. Verify that ComAgent links are established between DA-MPs under **Main Menu** > **Communication Agent** > **Maintenance**

3. Verify the No-MP Leader condition in **Main Menu** > **Diameter** > **Maintenance** > **DA-MPs** > **Peer DA-MP Status** that at least 1 DA-MP is MP-Leader.
4. If the problem persists, contact the *Customer Care Center*.

22062 - Actual Host Name cannot be determined for Topology Hiding

Event Type: Diameter

Description: Topology Hiding could not be applied because the Actual Host Name could not be determined

Severity: N/A

Instance: <CfgSetName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterTopoHidingActualHostNameNotFoundNotify

Recovery:

1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set.
2. If any DSR Applications are activated on DSR, ensure that any specific Application Level Topology Hiding feature is not conflicting with the contents of Actual Host Names specified in the MME Configuration Set.
3. Check if the first instance of a Session-ID AVP in the Request/Answer message contains the mandatory delimited ";".
4. If the problem persists, contact the *Customer Care Center*.

22101 - Connection Unavailable

Alarm Type: DIAM

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

Note: This alarm is not added when the "Suppress Connection Unavailable Alarm" for a Transport Connection is set to "Yes".

Severity: Major

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnectionUnavailableNotify

Recovery:

1. Identify the most recent Connection Unavailable event in the event log for the connection and use the Event's recovery steps to resolve the issue.
2. If the problem persists, contact the *Customer Care Center*.

22102 - Connection Degraded

Alarm Type: DIAM

Description: Connection is only available for routing messages with a priority greater than or equal to the connection's congestion level.

Severity: Major

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnectionDegradedNotify

Recovery:

1. Identify the most recent Connection Degraded event in the event log for the connection and use the Event's recovery steps to resolve the issue.
2. If the problem persists, contact the *Customer Care Center*.

22103 - SCTP Connection Impaired

Alarm Type: DIAM

Description: One or more paths of the SCTP connection went down.

Severity: Minor

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterSCTPConnectionImpairedAlarmNotify

Recovery:

1. Identify the most recent SCTP Connection Impaired event in the event log for the connection and use the Event's recovery steps to resolve the issue.
2. If the problem persists, contact the *Customer Care Center*.

22104 - SCTP peer is operating with a reduced IP address set

Alarm Type: DIAM

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

Severity: Minor

Instance: <TransConnName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterSCTPPeerReducedIPSetAlarmNotify

Recovery:

1. The peer is not able to advertise more than one IP address either due to an error in its configuration or due to being affected by a network interface failure. Check the networking configuration on the peer node.
2. If the problem persists, contact the *Customer Care Center*.

22106 - Ingress Message Discarded: DA-MP Ingress Message Rate Control

Alarm Type: DIAM

Description: An ingress message is discarded due to connection (or DA-MP) ingress message rate exceeding connection (or DA-MP) maximum ingress MPS.

Severity: Major

Instance: <MPHostName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIngressMessageDiscardedAlarmNotify

Recovery:

1. The ingress MPS on the DA-MP is exceeding the MP Maximum Ingress MPS. Consider decreasing the overall ingress message rate on the DA-MP by diverting the traffic or reducing the traffic.
2. If the problem persists, contact the *Customer Care Center* for assistance.

22200 - Local MP Congestion

Alarm Type: DIAM

Description: The Diameter Process is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterLocalMpCongestionNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of DIAMETER peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page.

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

3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

22201 - Ingress Message Rate

Alarm Type: DIAM

Description: The ingress message rate for the MP is approaching or exceeding its engineered traffic handling capacity.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIngressMessageRateNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If the problem persists, contact the *Customer Care Center*.

22202 - PDU Buffer Pool Utilization

Alarm Type: DIAM

Description: The MP's PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPDUBufferPoolUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

22203 - PTR Buffer Pool Utilization

Alarm Type: 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: eagleXgDiameterPtrBufferPoolUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined from the **Alarms & Events** page.

5. If the problem persists, contact the *Customer Care Center*.

22204 - Request Message Queue Utilization

Alarm Type: 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: eagleXgDiameterRequestMessageQueueUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the Request Task may be experiencing a problem preventing it from processing messages from its Request Message Queue. The alarm log should be examined from the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

22205 - Answer Message Queue Utilization

Alarm Type: 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:eagleXgDiameterAnswerMessageQueueUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the Answer Task may be experiencing a problem preventing it from processing messages from its Answer Message Queue. The alarm log should be examined from the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

22206 - Reroute Queue Utilization

Alarm Type: 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: eagleXgDiameterRerouteQueueUtilizationNotify

Recovery:

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer time-outs. The status of connections should be examined from the **Diameter** > **Maintenance** > **Connections** page.
2. If no additional congestion alarms are asserted, the Reroute Task may be experiencing a problem preventing it from processing messages from its Reroute Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If the problem persists, contact the *Customer Care Center*.

22207 - All-Connections Event Queue Utilization

Alarm Type: DIAM

Description: The MP's All-Connections Event Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress transactions will be rejected. This alarm should not normally occur when no other congestion alarms are asserted.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterAllConnectionsEventQueueUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage** > **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the task may be experiencing a problem preventing it from processing events from its All-Connections Event Queue. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

22208 - Per-Connection Egress Message Queue Utilization

Alarm Type: DIAM

Description: The MP's per-connection egress message queue is approaching its maximum capacity.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterPerConnMessageQueueUtilNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22215 - Ingress Message Discarded: DA-MP Overload Control

Alarm Type: DIAM

Description: Ingress message is discarded due to DA-MP CPU congestion

Severity: Major

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Auto Clear Seconds 0 (zero)

OID: eagleXgDiameterIngressMessageDiscardedOverLoadControlAlarmNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

22216 - Ingress Message Discarded: Priority 0 message discarded by DA-MP Overload Control

Alarm Type: DIAM

Description: Ingress Priority 0 message discarded due to DA-MP CPU congestion.

Severity: Info

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressPri0MessageDiscardedNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

22217 - Ingress Message Discarded: Priority 1 message discarded by DA-MP Overload Control

Alarm Type: DIAM

Description: Ingress Priority 1 message discarded due to DA-MP CPU congestion.

Severity: Info

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressPri1MessageDiscardedNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

22218 - Ingress Message Discarded: Priority 2 message discarded by DA-MP Overload Control

Alarm Type: DIAM

Description: Ingress Priority 2 message discarded due to DA-MP CPU congestion.

Severity: Info

Instance: MPHostName (Hostname of the DA-MP)

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressPri2MessageDiscardedNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

22220 - Connection Congestion Level change

Event Type: DIAM

Description: The egress congestion level associated with the connection has changed. When a connection's egress queue is congested, the connection's operational status will be Degraded. If this problem persists and the queue reaches 100% utilization all new egress messages for the Connection will be discarded. This event should not normally occur when no other congestion alarms are asserted.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterConnCongrestionLevelChangeNotify

Recovery:

1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.
4. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the *Customer Care Center*.

22221 - Routing MPS Rate

Alarm Type: DIAM

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

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterRoutingMPSRateNotify

Recovery:

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

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

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

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

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

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

4. If the problem persists, contact the *Customer Care Center*.

22222 - Long Timeout PTR Buffer Pool Utilization

Alarm Type: 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: eagleXgDiameterLongTimeoutPtrBufferPoolUtilizationNotify

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The misconfiguration of Pending Answer Timer assignment may result in excessive traffic being assigned to the Long Timeout PTR buffer Pool. View the Pending Answer Timer values via **Diameter** > **Configuration** > **Pending Answer Timers**. Examine the Pending Answer Timers

assignment via the **Diameter** > **Configuration** > **Application Ids and Diameter** > **Configuration** > **Peer Nodes**.

3. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second
4. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
5. A software defect may exist resulting in Long Timeout PTR buffers not being de-allocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log from **Main Menu** > **Alarms & Events**.
6. If the problem persists, contact the *Customer Care Center*

22223 - DA-MP Memory Utilization Exceeded

Alarm Type: DIAM

Description: DA-MP memory utilization has exceeded its configured limits.

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID eagleXgDiameterDampMemoryUtilizationExceededNotify

Recovery:

1. MPS exceeding its configured limits. Alarm *22221 - Routing MPS Rate* will be raised; perform the Recovery steps for this alarm.
2. Average hold time exceeding its configured limits. Alarm *22224 - Average Hold Time Limit Exceeded* will be raised. Perform the Recovery steps for this alarm.
3. Average message size exceeding its configured limits. Alarm *22225 - Average Message Size Limit Exceeded* will be raised. Perform the Recovery steps for this alarm.
4. Other. If the DA-MP is not exceeding any of the limits specified above, contact Oracle for assistance.

22224 - Average Hold Time Limit Exceeded

Alarm Type: DIAM

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

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID eagleXgDiameterAverageHoldTimeLimitExceededNotify

Recovery:

The average transaction hold time is exceeding its configured limits, resulting in an abnormally large number of outstanding transactions. Reduce the average hold time by examining the configured Pending Answer Timer values and reducing any values that are unnecessarily large.

22225 - Average Message Size Limit Exceeded

Alarm Type: DIAM

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

Severity: Minor, Major, Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID eagleXgDiameterAverageMessageSizeLimitExceededNotify

Recovery:

The size of the average message processed by DSR is exceeding its configured limits. This may cause DSR to consume an abnormally large amount of memory, leading to performance degradation. Alarm *22223 - DA-MP Memory Utilization Exceeded* may be raised as a result. Examine the traffic coming from connected peers to see if any of them are sending abnormally large messages.

22300 - Connection Unavailable: Socket configuration failure

Event Type: DIAM

Description: Software failure attempting to configure SCTP or TCP socket.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterConnUnavailSocketCfgFailureNotify

Recovery:

Contact the *Customer Care Center*.

22301 - Connection Unavailable: Connection initiation failure

Event Type: DIAM

Description: Failure occurred while attempting to initiate SCTP or TCP connection with the peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterConnUnavailConnInitFailureNotify

Recovery:

1. Confirm that connection is not administratively Disabled at the peer.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches local connection configuration.
3. Confirm IP network connectivity between peer IP and local IP for the connection.
4. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
5. If the problem persists, contact the *Customer Care Center*.

22302 - Connection Unavailable: Received malformed message

Event Type: DIAM

Description: Diameter message received from peer with invalid or inconsistent header/AVP length fields.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedMalformedMessageNotify

Recovery:

1. Determine if other nodes/MPs connected to the peer are also experiencing problems with messages received from the peer. If so, the peer should be diagnosed.
2. Determine if other connections on this same MP are also experiencing problems. If so, the MP should be removed moved from service, replaced, and the *Customer Care Center* should be contacted to assist with resolution.

22303 - Connection Unavailable: Peer closed connection

Event Type: DIAM

Description: The SCTP or TCP connection was closed by the peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailPeerClosedConnNotify

Recovery:

1. If unexpected, use peer node diagnostic/log information to determine why peer closed connection.
2. If the problem persists, contact the *Customer Care Center*.

22304 - Connection Unavailable: Proving Failure

Event Type: DIAM

Description: Connection closed after DWR/DWA based proving algorithm failure.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailProvingFailureNotify

Recovery:

1. Examine the peer to determine why it is not responding to DWRs.
2. If the problem persists, contact the *Customer Care Center*.

22305 - Connection Admin State change

Event Type: DIAM

Description: The Administrative state of the connection has changed.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnectionAdminStateChangeNotify

Recovery:

No action required.

22306 - Connection Unavailable: Timeout waiting for CER/CEA

Event Type: DIAM

Description: Connection closed after Tcex timer expired while waiting on CER or CEA from peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailTimedOutWaitingForCexNotify

Recovery:

1. For peer initiated connections, confirm that the configured Tcex timer value is not configured to be less than the expected time for peer to send CER after successfully initiating connection.
2. For locally initiated connections, confirm that the configured Tcex timer value is not less than the time expected for the peer to respond with CEA after receiving CER.
3. If the problem persists, contact the *Customer Care Center*.

22307 - Connection Unavailable: Timeout waiting for DPA

Event Type: DIAM

Description: Connection closed after Tdpa timer expired while waiting on DPA from peer.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailTimedOutWaitingForDpxNotify

Recovery:

No action required.

22308 - Received Unexpected CER/CEA

Event Type: DIAM

Description: CER or CEA message was received from the peer when it was not expected.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedUnexpectedCexNotify

Recovery:

1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact the *Customer Care Center*.

22309 - Received Unexpected DWR/DWA

Event Type: DIAM

Description: DWR or DWA message was received from the peer when it was not expected.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedUnexpectedDwxNotify

Recovery:

1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact the *Customer Care Center*.

22310 - Received Unexpected DPR/DPA

Event Type: DIAM

Description: DPR or DPA message was received from the peer when it was not expected.

Severity: Info

Instance: TransConnName

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedunexpectedDpxNotify

Recovery:

1. Diagnose peer for unexpected behavior.
2. If the problem persists, contact the *Customer Care Center*.

22311 - Invalid Diameter message received

Event Type: DIAM

Description: Diameter message received from peer which was decodable but contained a semantic error.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterReceivedinvalidDiameterMessageNotify

Recovery:

1. Analyze MsgOctets to determine which semantic error occurred and diagnose peer for unexpected behavior.
2. If the problem persists, contact the *Customer Care Center*.

22312 - Socket send failure

Event Type: DIAM

Description: An unexpected error occurred during the socket send call when attempting to send a Diameter message to the peer.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterFailedtoSendDiameterMessageNotify

Recovery:

1. Analyze error value to determine root cause.
2. If the problem persists, contact the *Customer Care Center*.

22313 - Connection Unavailable: Transport failure

Event Type: DIAM

Description: The connection was closed by the SCTP or TCP transport.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailtransportFailureNotify

Recovery:

1. Analyze error value to determine root cause.
2. If the problem persists, contact the *Customer Care Center*.

22314 - Connection Unavailable: CEA Realm/Host validation failure

Event Type: DIAM

Description: Origin-Realm and/or Origin-Host in CEA message received from peer on locally initiated connection does not match the locally configured connection.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailCeaRealmHostVldtnFailNotify

Recovery:

1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration using the **Diameter** > **Configuration** > **Local Nodes** page.
2. If the problem persists, contact the *Customer Care Center*.

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 the *Customer Care Center*.

22316 - Connection Unavailable: No common apps

Event Type: DIAM

Description: No common applications were found between local node and peer node during capabilities exchange.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailNoCommonAppsNotify

Recovery:

1. Reconcile Application IDs between local and peer nodes. If no common applications exist, the connection should be deleted or Disabled.
2. If the problem persists, contact the *Customer Care Center*.

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 the *Customer Care Center*.

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 the *Customer Care Center*.

22319 - Connection Unavailable: Diameter Watchdog

Event Type: DIAM

Description: Connection closed due to no traffic from peer within Tw*2 time after sending DWR.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavailWatchdogFailureNotify

Recovery:

1. Confirm that the connection is not administratively Disabled at the peer.
2. Confirm that the peer connection configuration (protocol, remote/local IP address, remote/local port) matches local connection configuration.

3. Confirm there is reliable IP network connectivity between the peer IP and the local IP for the connection (no excess packet loss).
4. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
5. If the problem persists, contact the *Customer Care Center*.

22320 - Invalid peer initiated connection

Event Type: DIAM

Description: Origin-Realm and or Origin-Host in CER message received or the peer IP addresses advertised on peer initiated connection does not match any locally configured connection

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterInvalidPeerInitdConnNotify

Recovery:

1. Confirm that peer connection configuration (Realm, Host, protocol, remote/local IP address, remote/local port) matches local connection configuration.
2. If the problem persists, contact the *Customer Care Center*.

22321 - Connection Unavailable: DNS Resolution Failure

Event Type: DIAM

Description: During connection initiation, Transport/Peer FQDN was unable to be resolved to an IP address via DNS

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnUnavilDnsResolutionFailureNotify

Recovery:

1. Confirm DNS is available and reachable by MP.
2. Confirm that DNS configuration contains peer FQDN and appropriate corresponding IP address(es).
3. Analyze errno value and text from Event Addn'l Info to determine root cause.
4. If the problem persists, contact the *Customer Care Center*.

22322 - Connection Proving Success

Event Type: DIAM

Description: The connection proving phase completed successfully.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnProvingSuccessNotify

Recovery:

No action required.

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 the *Customer Care Center*.

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 the *Customer Care Center*.

22326 - Connection Established

Event Type: DIAM

Description: The peer connection is available for signaling traffic.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterConnEstablishedNotify

Recovery:

No action required.

22327 - Initiator function disabled

Event Type: DIAM

Description: Peer disconnect reason indicated that we should not attempt to initiate a connection.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterInitiatorFunctionDisabledNotify

Recovery:

1. No action required. The peer can still initiate a connection. If the peer does not attempt to initiate a connection within a reasonable amount of time, the connection can be disabled, then re-enabled to re-activate the initiator function.
2. If the problem persists, contact the *Customer Care Center*.

22328 - Connection is processing a higher than normal ingress messaging rate

Alarm Group: DIAM

Description: The diameter connection specified in the alarm instance is processing a higher than normal ingress messaging rate.

Severity:

- Minor (if all of the following are true):

  - The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection minor alarm threshold.
  - The average ingress MPS rate that the connection is processing has not yet reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.
- Major (if the following are true):
  - The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

Instance: The name of the diameter connection as defined by the TransportConnection table.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameteringressMpsRateNotify

Recovery:

1. The Diameter connection specified in the Alarm Instance field is processing a higher than expected average ingress Diameter message rate. The alarm thresholds for minor and major alarms are configured in the Capacity Configuration Set used by the Diameter connection.
2. The message rate used for this alarm is an exponentially smoothed 30 second average. This smoothing limits false alarms due to short duration spikes in the ingress message rate.
3. If the alarm severity is minor, the alarm means that the average ingress message rate has exceeded the minor alarm threshold percentage of the maximum ingress MPS configured for the connection.
4. If the alarm severity is major, the alarm means that the average ingress message rate has exceeded the major alarm threshold percentage of the maximum ingress MPS configured for the connection.
5. This alarm is cleared when the average ingress message rate falls 5% below the minor alarm threshold, or the connection becomes disabled or disconnected. This alarm is downgraded from major to minor if the average ingress message rate falls 5% below the major alarm threshold.
6. If the average ingress message rate is determined to be unusually high, investigate the connection's remote Diameter peer (the source of the ingress messaging) to determine why they are sending the abnormally high traffic rate. Otherwise, consider increasing either the connection's maximum ingress MPS rate or the connection's alarm thresholds.

22329 - SCTP Connection Impaired: A path has become unreachable

Event Type: DIAM

Description: A path of an established SCTP connection has become unreachable.

Severity: Info

Instance: <TransConnName:Peer IP> (peer/remote IP of the failed path)

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterSctpConnectionImpairedNotify

Recovery:

1. Check whether the routing path between the local IP address and the peer IP address is up. If it is not, fix it.
2. If the problem persists, contact the *Customer Care Center*.

22330 - SCTP Connection Cfg Mismatch: The peer advertised a different number of IP addresses than configured

Event Type: DIAM

Description: The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterSctpConnectionxfgMismatchNotify

Recovery:

Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the **Diameter > Configuration > System Options** page.

22331 - SCTP Connection Partial Matching: SCTP connection accepted but the IP addresses advertised by the peer match only partially those configured for the peer in the connection object

Event Type: DIAM

Description: The peer has advertised in the INIT/INIT_ACK chunk a set of IP addresses which overlap but does not include all the IP addresses configured for the peer in the respective connection object.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterSCTPConnectionPartialMatchingNotify

Recovery:

1. Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the **Diameter > Configuration > System Options** page.
2. If the problem persists, contact the *Customer Care Center*.

22334 - Unexpected Message Priority in ingress Request

Event Type: DIAM

Description: The decoded Message Priority from the ingress Request has an unexpected value.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterUnexpMessagePriorityInRequestNotify

Recovery:

1. Verify that the peer is a DSR
   - Product-Name is reported as "Eagle XG DSR", in the Event Additional Information.
   - Vendor-Id is reported as 323 (Tekelec).
2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.
   - Call *Customer Care Center* and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   - If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call *Customer Care Center*.
   - If the reported Firmware-Version is less than the minimum required DSR software version, call *Customer Care Center* to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to "None".

22335 - Peer does not support Message Priority

Event Type: DIAM

Description: Cannot read Message Priority from ingress Requests because Peer does not support Message Priority.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterMessagePriorityNotSuppPeerNotify

Recovery:

1. Verify that the peer is a DSR
   - Product-Name is reported as "Eagle XG DSR", in the Event Additional Information.
   - Vendor-Id is reported as 323 (Tekelec).

2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.
   - Call *Customer Care Center* and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   - If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call *Customer Care Center*.
   - If the reported Firmware-Version is less than the minimum required DSR software version, call *Customer Care Center* to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to "None".

22343 - Connection Unavailable: Duplicate Connection Released

Event Type: DIAM

Description: Duplicate connection established, connection terminated.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterMpResIngressMpsOversubscribedNotify

Recovery:

No action necessary.

22344 - Failed to process ingress message: Processor Unavailable or Congested

Event Type: DIAM

Description: The message processor is Unavailable or Congested. This event refers to another DA-MP, not the one reporting the problem.

Severity: Info

Instance: <SourceMpHost>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterProcessorUnavlblOrCngstedNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22345 - Connection Priority Level changed

Event Type: DIAM

Description: The Diameter Connection's CPL has transitioned from its current value to a new CPL value based on congestion levels reported by various features.

Severity: Info

Instance: <TransConnName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterCplChangedNotify

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Identify the most recent "Connection Degraded" event in the event log for the connection and utilize the Event Detailed information to diagnose the condition.
3. If the problem persists, contact the *Customer Care Center* for assistance.

22346 - MP Reserved Ingress MPS Oversubscribed

Event Type: DIAM

Description: The total connection Reserved Ingress MPS exceeds the Engineered Ingress MPS capacity of the MP.

Severity: Info

Instance: MPName (Hostname of the DA-MP Server)

HA Score: Normal

Throttle Seconds: 1

OID: eagleXgDiameterMpResIngressMpsOversubscribedNotify

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Perform one or more of these actions:
   - Increase the maximum reserved capacity by increasing the value of IPFE Connection Reserved Ingress MPS Scaling parameter.
   - Reduce the subscribed amount of reserved capacity by reducing the number of connections.
   - Reduce the reserved capacity required by connections.
3. If the problem persists, contact the *Customer Care Center* for assistance.

22347 - Ingress Message Discarded: DA-MP shared ingress capacity exhausted

Alarm Type: DIAM

Description: An ingress message is discarded on a DA-MP due to the ingress message rate on the DA-MP exceeding MP Maximum Ingress MPS.

Severity: N/A

Instance: <MPHostName>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterMpIngressMessageDiscardedNotify

Recovery:

1. The ingress MPS on the DA-MP is exceeding the MP Maximum Ingress MPS. Consider decreasing the overall ingress message rate on the DA-MP by diverting the traffic or reducing the traffic.
2. If the problem persists, contact the *Customer Care Center* for assistance.

22349 - IPFE Connection Alarm Aggregation Threshold

Alarm Type: DIAM

Description: This alarm occurs when there are a 'Critical' number of IPFE Connection alarms for the Network Element.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical, Major

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

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterIPFEConnUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Connection** to monitor IPFE Connection status.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
4. Verify that the peers in the Route List are not under maintenance.
5. Contact the *Customer Care Center* for assistance.

22350 - Fixed Connection Alarm Aggregation Threshold

Alarm Type: DIAM

Description: This alarm occurs when there are a 'Critical' number of Fixed Connection alarms for the DA-MP.

Note: The Alarm Thresholds are configurable using the "Alarm Threshold Options" tab on the **Main Menu** > **Diameter** > **Configuration** > **System Options** screen.

Severity: Critical, Major

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

Instance: <DA-MP-Hostname>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterFixedConnUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Connection** to monitor Fixed Connection status.
2. Confirm that peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm that the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
4. Verify that the peers in the Route List are not under maintenance.
5. Contact the *Customer Care Center* for assistance.

22900 - DPI DB Table Monitoring Overrun

Event Type: DIAM

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

Severity: Info

Instance: <DbTblName>

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

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterDpiTblMonCbOnLogOverrunNotify

Recovery:

Contact the *Customer Care Center* 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:eagleXgDiameterDpSldbMonAbnormalErrorNotify

Recovery:

Contact the *Customer Care Center*.

22950 - Connection Status Inconsistency Exists

Alarm Type: DIAM

Description: Diameter Connection status inconsistencies exist among the DA-MPs in the DSR signaling NE.

Severity: Critical

Instance: <MpName> (where inconsistency detected)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterConnectionStatusInconsistencyNotify

Recovery:

No action necessary.

Note: DA-MP's SLDB tables are automatically audited and re-synchronized to correct inconsistencies after a log overrun has occurred.

22960 - DA-MP Profile Not Assigned

Alarm Type: DIAM

Description: A DA-MP configuration profile has not been assigned to this DA-MP.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDaMpProfileNotAssignedNotify

Recovery:

1. A DA-MP profile must be assigned to the DA-MP via the DSR OAM GUI.
2. If the problem persists, contact the *Customer Care Center*.

22961 - Insufficient Memory for Feature Set

Alarm Type: DIAM

Description: The Available Memory (in kilobytes) for Feature Set is less than the Required Memory (in kilobytes).

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterInsufficientAvailMemNotify

Recovery:

1. Make additional memory available on the DA-MP for the configured DiameterMaxMessageSize.
2. If the problem persists, contact the *Customer Care Center*.

Range Based Address Resolution (RBAR) Alarms and Events (22400-22424)

22400 - Message Decoding Failure

Event Type: RBAR

Description: A message received was rejected because of a decoding failure.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarMsgRejectedDecodingFailureNotify

Recovery:

While parsing the message, the message content was inconsistent with the Message Length in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

22401 - Unknown Application ID

Event Type: RBAR

Description: A message could not be routed because the Diameter Application ID is not supported.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarUnknownApplIdNotify

Recovery:

1. The DSR Relay Agent forwarded a Request message to the address resolution application which contained an unrecognized Diameter Application ID in the header. Either a DSR Relay Agent application routing rule is mis-provisioned or the Application ID is not provisioned in the RBAR routing configuration.
2. View the currently provisioned Diameter Application IDs by selecting **RBAR** > **Configuration** > **Applications**.
3. View the currently provisioned Application Routing Rules by selecting **Diameter** > **Configuration** > **Application Routing Rules**.

22402 - Unknown Command Code

Event Type: RBAR

Description: A message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarUnknownCmdCodeNotify

Recovery:

1. The order pair (Application ID, Command Code) is not provisioned in the Address Resolutions routing configuration.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22403 - No Routing Entity Address AVPs

Event Type: RBAR

Description: A message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarNoRoutingEntityAddrAvpNotify

Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22404 - No valid Routing Entity Addresses found

Event Type: RBAR

Description: A message could not be routed because none of the address AVPs contained a valid address and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarNoValidRoutingEntityAddrFoundNotify

Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22405 - Valid address received didn't match a provisioned address or address range

Event Type: RBAR

Description: A message could not be routed because a valid address was found that did not match an individual address or address range associated with the Application ID, Command Code, and Routing Entity Type, and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddressResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarAddrMismatchWithProvisionedAddressNotify

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.

2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

22406 - Routing attempt failed due to internal resource exhaustion

Event Type: RBAR

Description: A message could not be routed because the internal "Request Message Queue" to the DSR Relay Agent was full. This should not occur unless the MP is experiencing local congestion as indicated by Alarm-ID *22200 - Local MP Congestion*.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarRoutingAttemptFailureinternalResExhNotify

Recovery:

If this problem occurs, contact the *Customer Care Center*.

22407 - Routing attempt failed due to internal database inconsistency failure

Event Type: RBAR

Description: A message could not be routed because an internal address resolution run-time database inconsistency was encountered.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterRbarRoutingFailureInternalDbInconsistencyNotify

Recovery:

If this problem occurs, contact the *Customer Care Center*.

Generic Application Alarms and Events (22500-22599)

Note: These alarms are generic across the various DSR applications with some details varying depending on the application generating the alarm.

22500 - DSR Application Unavailable

Alarm Type: APPL

Description: DSR Application is unable to process any messages because it is Unavailable

Severity: Critical

Instance: <DSR Application Name>

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDSRApplicationUnavailableNotify

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify that the Admin State is set as expected.
2. A DSR Application operation status becomes Unavailable when either the Admin State is set to Disable with the Forced Shutdown option, or the Admin State is set to Disable with the Graceful Shutdown option and the Graceful Shutdown timer expires.
3. A DSR Application can also become Unavailable when it reaches Congestion Level 3 if enabled.

   Note: This alarm will NOT be raised when the DSR application is shutting down gracefully or application is in Disabled state. Only the DSR Application operational status will be changed to Unavailable.

4. Check the Event History logs for additional DIAM events or alarms for this MP server.
5. If the problem persists, contact the *Customer Care Center*.

22501 - DSR Application Degraded

Alarm Type: APPL

Description: Unable to forward requests to the DSR Application because it is Degraded

Severity: Major

Instance: <DSR Application Name>

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDSRApplicationDegradedNotify

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify that the Admin State is set as expected.
2. A DSR Application becomes Degraded when the DSR Application becomes congested if enabled.

Note: This alarm will NOT be raised when the DSR application is shutting down gracefully or application is in Disabled state. Only the DSR Application operational status will be changed to Unavailable.

3. Check the Event History logs for additional DIAM events or alarms for this MP server.
4. If the problem persists, contact the *Customer Care Center*.

22502 - DSR Application Request Message Queue Utilization

Alarm Type: APPL

Description: The DSR Application Request Message Queue Utilization is approaching its maximum capacity

Severity:

- **Minor:** Request Queue utilization becomes over 60%
- **Major:** Request Queue utilization becomes over 80%
- **Critical:** Request Queue utilization becomes over 95%

Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraRequestMsgQueue, RxCpaRequestMsgQueue for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDSRAppRequestMessageQueueUtilizationNotify

Recovery:

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

   The DSR Application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.
2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
3. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Request Message Queue. Examine the Alarm log in **Alarms & Events**
4. If the problem persists, contact the *Customer Care Center*.

22503 - DSR Application Answer Message Queue Utilization

Alarm Type: APPL

Description: The DSR Application Answer Message Queue Utilization is approaching its maximum capacity.

Severity:

- **Minor:** Answer Queue utilization becomes over 60%
- **Major:** Answer Queue utilization becomes over 80%
- **Critical:** Answer Queue utilization becomes over 95%

Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraAnswerMsgQueue, RxCpaAnswerMsgQueue for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDSRAppAnswerMessageQueueUtilizationNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules** in the SO GUI.
2. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Answer Message Queue. Examine the Alarm log in **Alarms & Events**
3. If the problem persists, contact the *Customer Care Center*.

22504 - DSR Application Ingress Message Rate

Alarm Type: APPL

Description: The ingress message rate for the DSR Application is exceeding its engineered traffic handling capacity.

Severity:

- **Minor:** Ingress Message Rate becomes over 110% of the ingress message capacity
- **Major:** Ingress Message Rate becomes over 140% of the ingress message capacity
- **Critical:** Ingress Message Rate becomes over 160% of the ingress message capacity

Instance: <Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm will vary (RxPdraMsgRate, RxCpaMsgRate for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterDSRAppIngressMessageRateNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules** in the SO GUI.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, contact the *Customer Care Center*.

25510 - Multiple DA-MP Leader Detected Alarm

Alarm Type: DIAM

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

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMultipleDaMpLeadersDetectedNotify

Recovery:

If the problem persists, contact the *Customer Care Center* for assistance.

22520 - DSR Application Enabled

Event Type: APPL

Description: DSR Application Admin state was changed to 'enabled'.

Severity: Info

Instance: <DSR Application Name>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationEnabledNotify

Recovery:

No action required.

22521 - DSR Application Disabled

Event Type: APPL

Description: DSR Application Admin state was changed to 'disabled'.

Severity: Info

Instance: <DSR Application Name>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterDsrApplicationDisabledNotify

Recovery:

No action required.

Full Address Based Resolution (FABR) Alarms and Events (22600-22640)

22600 - Message Decoding Failure

Event Type: FABR

Description: Message received was rejected because of a decoding failure. While parsing the message, the message content was inconsistent with the "Message Length" in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message), the peer who forwarded the message to this node, or any intermediate node that modifies the message.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrMsgRejectedDecodingFailureNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22601 - Unknown Application ID

Event Type: FABR

Description: Message could not be routed because the Diameter Application ID is not supported.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrUnknownApplIdNotify

Recovery:

A Request message was forwarded to the FABR application which contained an unrecognized Diameter Application ID in the header. Either an application routing rule is mis-provisioned or the Application ID is not provisioned in the FABR configuration.

1. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**
2. The currently provisioned Diameter Application IDs can be viewed in the **FABR** > **Configuration** > **Applications Configuration**.
3. Contact the *Customer Care Center* for assistance.

22602 - Unknown Command Code

Event Type: FABR

Description: Message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrUnknownCmdCodeNotify

Recovery:

Either an application routing rule is mis-provisioned or the Command Code is not provisioned in the FABR configuration.

1. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**
2. The currently provisioned Diameter Application IDs can be viewed in the **FABR** > **Configuration** > **Address Resolutions**.
3. Contact the *Customer Care Center* for assistance.

22603 - No Routing Entity Address AVPs

Event Type: FABR

Description: Message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrNoValidUserIdentityAddrAvpNotify

Recovery:

1. If this event is considered abnormal, then validate which AVPs are configured for routing with the Application ID and Command Code using **FABR** > **Configuration** > **Address Resolutions**.
2. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**
3. Contact the *Customer Care Center* for assistance.

22604 - No valid User Identity Addresses found

Event Type: FABR

Description: No valid User Identity Address is found in the configured AVPs contained in the ingress message.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrNoValidUserIdentityAddrFoundNotify

Recovery:

1. If this event is considered abnormal, then validate which AVPs are configured for routing with the Application ID and Command Code using **FABR** > **Configuration** > **Address Resolutions**.
2. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**
3. Contact the *Customer Care Center* for assistance.

22605 - No Destination address is found to match the valid User Identity address

Event Type: FABR

Description: Message could not be routed because the valid user identity address extracted from the message did not resolve to a destination address. The Routing Exception was configured to send an Answer response. Please verify the provisioning in the address resolution table and the data provided in the SDS corresponding to this address/resolution entry.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrNoAddrFoundAtDpNotify

Recovery:

The FABR address resolution table entry may be misconfigured or the destination address associated with User Identity address from the message and the destination type configured in the address resolution table may be missing from the address mapping configuration. The destination address associated with User Identity address derived may be missing from the address mapping configuration on DP/SDS.

1. Validate the address resolution table entry and verify that a valid destination address is associated with the user identity address by using DP configuration.

   For additional information, see Subscriber Database Server online help.

2. Contact the *Customer Care Center* for assistance.

22606 - Database or DB connection error

Event Type: FABR

Description: FABR application receives service notification indicating Database (DP) or DB connection (ComAgent) Errors (DP timeout, errors or ComAgent internal errors) for the sent database query.

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrDpErrorsNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22607 - Routing attempt failed due to DRL queue exhaustion

Event Type: FABR

Description: Message could not be routed because the internal "Request Message Queue" to the DSR Relay Agent was full.

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrRoutingAttemptFailureDrlQueueExhNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22608 - Database query could not be sent due to DB congestion

Event Type: FABR

Description: FABR could not send a database query either because the ComAgent reported DP congestion level of (CL=2 or 3), or an abatement period is in progress.

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrDpCongestedNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22609 - Database connection exhausted

Event Type: FABR

Description: Database queries could not be sent because the database connection (ComAgent) queue was full

Severity: Info

Instance: <MPNname>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrDbConnectionExhNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22610 - FABR DP Service congestion state change

Event Type: FABR

Description: FABR application received status notification indicating DP congestion state change or DP congestion abatement time period has completed.

Severity: Info

Instance: <MPName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: eagleXgDiameterFabrdpCongestionStateChangeNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22611 - FABR Blacklisted Subscriber

Event Type: FABR

Description: Message could not be routed because valid User Identity Address extracted from diameter request belongs to blacklisted subscriber.

Severity: Info

Instance: <AddrResolution>

HA Score: Normal

Throttle Seconds: 10

OID: eagleXgDiameterFabrBlacklistedSubscriberNotify

Recovery:

The destination address associated with User Identity address derived is blacklisted in the address mapping configuration on DDR.

1. Validate which User identity address is not blacklisted by using DP configuration.
2. If the problem persists, contact the *Customer Care Center*.

22631 - FABR DP Response Task Message Queue Utilization

Alarm Type: FABR

Description: The FABR Application's DP Response Message Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxFabrDpResponseMsgQueue, FABR

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterFabrAppDpResponseMessageQueueUtilizationNotify

Recovery:

1. This alarm may occur due to persistent overload conditions with respect to database response processing.
2. Contact the *Customer Care Center* for assistance.

22632 - COM Agent Registration Failure

Alarm Type: FABR

Description: The Communication Agent routing service registration or service notification registration failed, FABR can not use the Communication Agent service for database queries.

Severity: Critical

Instance: Full Address Based Resolution

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterComAgentRegistFailNotify

Recovery:

Contact the *Customer Care Center* for assistance.

Policy DRA (PDRA) Alarms and Events (22700-22799)

22700 - Protocol errors in Diameter Requests

Event Group: PDRA

Description: The Diameter request message(s) received by Policy DRA contain protocol error(s).

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraProtocolErrorsInDiameterReqNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22701 - Protocol errors in Diameter Answers

Event Group: PDRA

Description: The Diameter answer message(s) received by Policy DRA contain(s) protocol error(s). The Error Message is based on the specific error scenario.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraProtocolErrorsInDiameterAnsNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22703 - Diameter message routing failure due to DRL queue exhaustion

Event Type: PDRA

Description: The Diameter egress message (request or answer) could not be sent due to DRL queue exhaustion.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraEgressMsgRoutingFailureDueToDrlQueueExhaustedNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22704 - Policy DRA Communication Agent Error

Event Type: PDRA

Description: A communication failure occurs between the Policy DRA server and the Policy SBR server.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraStackEventSendingFailureCAUnavailNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22705 - Policy SBR Error Response Received By Policy DRA

Event Type: PDRA

Description: The Policy DRA server received a response from the Policy SBR server indicating Policy SBR errors.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraPsbrErrorIndicationNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22706 - Binding Key Not Found In Diameter Message

Event Type: PDRA

Description: A binding key is not found in the received CCR-I message.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraBindingKeyNotFoundNotify

Recovery:

1. Check the P-DRA GUI at **Policy DRA** > **Configuration** > **Binding Key Priority**.
2. Contact the *Customer Care Center* for assistance

22707 - Policy DRA Diameter Message Processing Failure

Alarm Type: PDRA

Description: The Policy DRA failed to process a Diameter message. The specific reason is provided by the Policy DRA signaling code.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraDiameterMessageProcessingFailureNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22710 - Policy SBR Sessions Threshold Exceeded

Alarm Type: pSBR

Description: The number of sessions threshold for a Policy DRA Mated Sites Place Association has been exceeded.

Severity:

- **Minor**: pSBR session numbers are greater than or equal to 80% of maximum session capacity
- **Major**: pSBR session numbers are greater than or equal to 90% of maximum session capacity
- **Critical**: pSBR session numbers are greater than or equal to 95% of maximum session capacity

Instance: Policy DRA Mated Sites Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrActSessThreshNotify

Recovery:

1. Determine if the alarm thresholds for Session Capacity are properly configured on the PDRA Network OAM GUI Main Menu from **Policy DRA** > **Configuration** > **Alarm Settings**. Alarm severity is determined by the number of session records stored in in the policy session database exceeding the alarm threshold percentage of the calculated session capacity for the topology.
2. If the alarm assert thresholds are improperly configured, they can be configured on a network-wide basis from the Network OAM Gui Main menu from **Policy DRA** > **Configuration** > **Alarm Settings**.
3. In general, the system should be sized to host the expected number of concurrent sessions per policy subscriber.
4. If the system is nearing 100% capacity, contact the *Customer Care Center* for further assistance.

22711 - Policy SBR Database Error

Alarm Type: pSBR

Description: An error occurred during a Policy SBR database operation.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: cAFPSBRDbOpFailNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22712 - Policy SBR Communication Error

Alarm Type: pSBR

Description: The Policy SBR received an error or timeout response from Communication Agent.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: cAFPSBRStkEvFailComAgentNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22713 - Policy SBR Alternate Key Creation Error

Alarm Type: pSBR

Description: An attempt to create an Alternate Key record in the Binding database failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: cAFPSBRAltKeyCreateFailNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22714 - Policy SBR RAR Initiation Error

Alarm Type: pSBR

Description: Policy SBR encountered an error while processing Policy DRA initiated RAR requests.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: cAFPSBRRARInitiationErrNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22715 - Policy SBR Audit Suspended

Alarm Type: pSBR

Description: This alarm indicates that Policy SBR binding and/or session auditing has been suspended due to a congestion condition on either the local server reporting the alarm, or on a remote server being queried for auditing purposes.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSBRAuditSuspendedNotify

Recovery:

1. The Policy SBR audit cleans up stale records in the database. Prolonged suspension of the audit could result in the exhaustio of memory resources on a binding or session Policy SBR server. Investigate the causes of congestion on the Policy SBR servers (see also Alarm *22725 - Policy SBR Server In Congestion*).
2. If the problem persists, contact the *Customer Care Center*.

22716 - Policy SBR Audit Statistics Report

Event Group: pSBR

Description: This report provides statistics related to Policy SBR session or binding table audits. Each Policy SBR server generates this event upon reaching the last record in a table. The statistics reported are appropriate for the type of table being audited.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (no throttling)

OID: cAFPSBRAuditStatisticsReportNotify

Recovery:

Contact the *Customer Care Center*.

22717 - Policy SBR Alternate Key Creation Failure Rate

Alarm Type: pSBR

Description: Policy SBR Alternate Key Creation Failure rate exceeds threshold.

Severity: Minor, Major, Critical

Instance: PDRA Mated Pair Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPsbrAltKeyCreationFailureRateNotify

Recovery:

1. Check ComAgent Congestion alarms on the Binding PSBRs. If the Binding PSBRs are congested, it is likely that there is a very high rate of Diameter traffic.
2. Check the ComAgent connections statuses. This issue can occur if the ComAgent connections between the Session and Binding PSBRs are not "In Service". ComAgent connection statuses can be found on the Active NOAMP GUI at **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status**.
3. If any of the connections are disabled, change the administratice state to enabled. If any connections are enabled but not "In Service", there could be a network issue.
4. If the further assistance is needed, contact the *Customer Care Center*.

22718 - Binding Not Found for Binding Dependent Session Initiate Request

Event Group: PDRA

Description: Binding record is not found for the configured binding keys in the binding dependent session-initiation request message.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: pdraPdraBindingNotFoundBindingDependentNotify

Recovery:

1. Check the PDRA GUI Main Menu **Policy DRA** > **Configuration** > **Binding Key Priority** on the subscriber key priorities to ensure the configuration is correct.
2. Using the Binding Key Query Tool, check if a binding exists for the binding keys at **Policy DRA** > **Configuration** > **Binding Key Priority**.

22719 - Maximum Number of Sessions per Binding Exceeded

Event Group: pSBR

Description: The maximum number of sessions per binding is exceeded that fails the attempt to create a binding for a given subscriber key

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 60

OID: cAfPSBRMaxSessionPerBindingExceededNotify

Recovery:

1. Determine if the existing sessions are valid. The existing sessions may be displayed using the Binding Key Query Tool to obtain all relevant information including session-ids and PCEF FQDNs.
2. If the sessions exist in the P-DRA but not on the PCEF(s), call the *Customer Care Center*.

22720 - Policy SBR To Policy DRA Response Queue Utilization Threshold Exceeded

Alarm Type: PDRA

Description: The Policy DRA's pSBR Response Queue threshold has been exceeded.

Severity:

- **Minor**: pSBR Response Queue Utilization becomes over 60%
- **Major**: pSBR Response Queue Utilization becomes over 80%

- **Critical**: pSBR Response Queue Utilization becomes over 95%

Instance: RxPdraSbrEventMsgQueue, Policy DRA

HA Score: Normal

OID: pdraPdraPsbrResponseQueueUtilizationNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**

   Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, contact the *Customer Care Center*.

22721 - Policy DRA Server In Congestion

Alarm Type: PDRA

Description: The operational state of the Policy DRA is congested.

Severity:

- **Minor**: ingress Request rate is 110% of PR-MPS or larger
- **Major**: ingress Request rate is 140% of PR-MPS or larger
- **Critical**: ingress Request rate is 160% of PR-MPS or larger

Instance: Policy DRA

HA Score: Normal

OID: pdraPdraCongestionStateNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, contact the *Customer Care Center*.

22722 - Policy DRA Binding Sub-resource Unavailable

Alarm Type: PDRA

Description: One or more of the binding sub-resources are not available.

Severity:

- **Major**: When at least one of the binding sub-resources is not available
- **Critical**: When all of the binding sub-resources is not available

Instance: Policy DRA

HA Score: Normal

OID: pdraPdraBindingSubresourceUnavailableNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Monitor the P-DRA Binding Resource on the P-DRA Network OAM at **Main Menu** > **Configuration** > **Resource Domains**
2. If the problem persists, contact the *Customer Care Center*.

22723 - Policy DRA Session Sub-resource Unavailable

Alarm Type: PDRA

Description: One or more of the session sub-resources are not available.

Severity:

- **Major**: When at least one of the server groups hosting session sub-resources is not available
- **Critical**: When all of the server groups hosting session sub-resources are not available

Instance: Policy DRA

HA Score: Normal

OID: pdraPdraSessionSubresourceUnavailableNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Monitor the P-DRA Session Resource at **Main Menu** > **Configuration** > **Resource Domains**
2. If the problem persists, contact the *Customer Care Center*.

22724 - Policy SBR Memory Utilization Threshold Exceeded

Alarm Type: pSBR

Description: The Policy SBR server memory utilization threshold has been exceeded.

Severity:

- **Minor**: pSBR memory utilization threshold exceeds 70%

- **Major**: pSBR memory utilization threshold exceeds 80%
- **Critical**: pSBR memory utilization threshold exceeds 90%

Instance: Policy DRA Mated Sites Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrMemUtilNotify

Recovery:

1. If this condition persists, it may be necessary to allocate more memory for pSBR.
2. Contact the *Customer Care Center* for further assistance.

22725 - Policy SBR Server In Congestion

Alarm Type: pSBR

Description: The Policy SBR server is operating in congestion.

Severity:

- **Minor:** CL_1
- **Major:** CL_2
- **Critical:** CL_3

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrServerInCongestionNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Main Menu** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, contact the *Customer Care Center*.

22726 - Policy SBR Queue Utilization Threshold Exceeded

Alarm Type: pSBR

Description: The Policy SBR queue utilization has reached the configured threshold values.

Severity:

- **Minor**: pSBR stack event queue utilization threshold exceeds 60%
- **Major**: pSBR stack event queue utilization threshold exceeds 80%
- **Critical**: pSBR stack event queue utilization threshold exceeds 95%

Instance: Policy DRA Mated Sites Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrStackEvQUtilNotify

Recovery:

1. If this condition persists, it may be necessary to allocate larger queue sizes.
2. Contact the *Customer Care Center* for further assistance.

22727 - Policy SBR Initialization Failure

Alarm Type: pSBR

Description: The Policy SBR server psbr process failed to initialize.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrInitializationFailureNotify

Recovery:

Contact the *Customer Care Center* for further assistance.

22728 - Policy SBR Bindings Threshold Exceeded

Alarm Type: pSBR

Description: The number of Policy SBR bindings threshold has been exceeded.

Severity:

- **Minor**: pSBR active bindings threshold is greater than or equal to 80% of maximum binding capacity
- **Major**: pSBR active bindings threshold is greater than or equal to 90% of maximum binding capacity
- **Critical**: pSBR active bindings threshold is greater than or equal to 95% of maximum binding capacity

Instance: PDRA Binding Region Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrActBindThreshNotify

Recovery:

1. Determine if alarm thresholds for Binding Capacity are properly configured on the PDRA Network OAM GUI Main Menu from **Policy DRA** > **Configuration** > **Alarm Settings**.
   Alarm severity is determined by the number of binding records stored in the Binding Region exceeding the alarm threshold percentage of the calculated binding capacity for the topology.

2. If the alarm assert thresholds are improperly configured, they can be configured on a network-wide basis from the Network OAM Gui Main menu from **Policy DRA** > **Configuration** > **Alarm Settings**.
3. In general, the system should be sized to host 1 binding per policy subscriber.
4. If the system is nearing 100% capacity, contact the *Customer Care Center* for further assistance.

22729 - PCRF Not Configured

Alarm Type: PDRA

Description: PCRFs connected to the Policy DRA are not configured.

Severity: Critical

Instance: Policy DRA

HA Score: Normal

OID: pdraPcrfNotConfiguredNotify

Auto Clear Seconds: 0 (zero)

Recovery:

1. Check the P-DRA GUI at **Main Menu** > **Policy DRA** > **Configuration** > **PCRFs** for further PCRF configuration.
2. Check the event history logs in **Alarms & Events**.
3. If the problem persists, contact the *Customer Care Center*.

22730 - Policy DRA Configuration Error

Alarm Group: PDRA

Description: Policy message processing could not be successfully completed due to a configuration error.

Severity: Major

Instance: "Unconfigured PCRF", "Unconfigured APN", "Missing APN", or "No Configured PCRFs"

HA Score: Normal

OID: pdraPdraConfigErrorNotify

Auto Clear Seconds: 300

Recovery:

1. If there is an unconfigured PCRF, it means that the binding capable session initiation request was routed to a PCRF that is not configured in **Policy DRA** > **Configuration** > **PCRFs** at the site where the request was received. This indicates a mismatch between the PCRF's configuration and the routing configuration. If the PCRF is a valid choice for the request, configure the PCRF in **Policy DRA** > **Configuration** > **PCRFs**. If the PCRF is not valid for the request, correct the routing table or tables that included the PCRF.

   See also *RxBindCapUnknownPcrf*.
2. If there is an unconfigured APN and if the APN string is valid, configure the APN at the NOAMP using the **Policy DRA** > **Configuration** > **Access Point Names** screen. If the APN string is not

valid, investigate the policy client to determine why it is sending policy session initiation requests using the invalid APN.

See also *RxBindCapUnknownApn* and *RxBindDepUnknownApn*.

3. If there is a missing APN, investigate the policy client to determine why it is sending policy session initiation requests with no APN.

   See also *RxBindCapMissingApn* and *RxBindDepMissingApn*

4. If there are no PCRFs configured, configure PCRFs at the SOAM GUI for the site using **Policy DRA** > **Configuration** > **PCRFs**.
5. Contact the *Customer Care Center*

22731 - Policy DRA Database Inconsistency

Alarm Type: PDRA

Description: The Policy DRA Database data inconsistency exists due to an internal error such as table truncation, code error etc.

Severity: Major

Instance: Policy DRA

HA Score: Normal

Auto Clear Seconds: 60

OID: pdraPdraDbInconsistencyExistsNotify

Recovery:

1. Check the error history logs for the details of the data inconsistency.
2. If the problem persists, contact the *Customer Care Center*.

22732 - Policy SBR Process CPU Utilization Threshold Exceeded

Alarm Type: pSBR

Description: The Policy SBR process on the indicated server is using higher than expected CPU resources.

Severity:

- **Minor**: pSBR process CPU utilization threshold exceeds 60%
- **Major**: pSBR process CPU utilization threshold exceeds 66%
- **Critical**: pSBR process CPU utilization threshold exceeds 72%

Instance: Policy DRA Mated Sites Place Association

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPSbrProcCpuThreshNotify

Recovery:

1. If this condition persists, it may be necessary to deploy more policy signaling capacity.

2. Contact the *Customer Care Center* for further assistance.

22733 - Policy SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration

Alarm Group: pSBR

Description: The Policy SBR failed to free binding memory after PCRF Pooling binding migration.

Severity: Minor

Instance: None

HA Score: Normal

Auto Clear Seconds: 0

OID: cAFPsbrPostMigrationMemFreeNotify

Recovery:

1. On systems upgraded from a release where Policy DRA was running, but that did not support PCRF Pooling, to a release that supports PCRF Pooling, binding data is migrated from the tables used by the old release to tables used by the new release. Once this migration process completes on a given binding policy SBR, a script is automatically executed to free memory for the old tables. If this script should fail for any reason to free the memory, this alarm is asserted.
2. If additional assistance is needed, contact the *Customer Care Center*.

22734 - Policy DRA Unexpected Stack Event Version

Alarm Group: PDRA

Description: A server upgrade discovers an unexpected stack event library version because one of the following occurs:

- An attempt is made to send a current version stack event, but the sender is informed that the target server only supports the old version.
- An old version stack event is received after all servers should have been upgraded to support the new version

Severity: Major

Instance: None

HA Score: Normal

OID: pdraPdraUnexpectedSEDownVersionNotify

Auto Clear Seconds: 300

Recovery:

1. From the NOAMP GUI at **Policy DRA** > **Maintenance** > **Policy SBR Status**, Find the Resource Domain Name to which the stack event was being sent.
2. Expand all Server Groups having that Resource Domain name to see which Server Group hosts the ComAgent Sub Resource.

3. The Server with Resource HA Role of "Active" is likely the server that has the old software (unless a switch-over has occurred since the alarm was asserted). In any case, one of the servers in the Server Group has old software. The software version running on each server can be viewed from **Administration** > **Upgrade**. The "Hostname" field is the same as the Server Name on the Policy SBR Status screen
4. Find the server or servers running the old software and upgrade those servers to the current release and accept the upgrade.
5. If additional assistance is needed, contact the *Customer Care Center*.

Charging Proxy Application (CPA) Alarms and Events (22800-22849)

22804 - Number of cSBR Unavailable Subresources at Threshold

Alarm Type: CPA

Description: The number of unavailable SBR subresources meets or exceeds the CpaSbrForUnavailable engineering configurable threshold.

Severity: Critical

Instance: Site Id

HA Score: Normal

Auto Clear Seconds: N/A

OID: eagleXgDiameterCpaUnavailableSubresourcesAtThreshold

Recovery:

1. Check the state of the SBR MPs.

   One or more Charging SBR subresources are unavailable. Make sure the SBR MPs are not having networking trouble.

2. Contact the *Customer Care Center* for assistance.

22805 - Message Decoding Failure

Event Type: CPA

Description: The CPA application could not decode a received Diameter message

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaMsgDecodeFailureNotify

Recovery:

1. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

   While parsing the message, the message content was inconsistent with the "Message Length" in the message header.

2. Contact the *Customer Care Center* for assistance.

22806 - Unknown Diameter Application Id

Event Type: CPA

Description: The CPA application received a Diameter message with an unexpected DSR application id. The DSR Relay Agent forwarded a Request message to the CPA application which contained an unrecognized Diameter Application ID in the header. A DSR Relay Agent application routing rule is mis-provisioned.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnkownAppIdNotify

Recovery:

1. Examine the DSR Relay Agent application routing rule for provisioning errors.

   The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.

2. Contact the *Customer Care Center* for assistance.

22807 - Unknown Command Code

Event Type: CPA

Description: The CPA application received a Diameter message other than an Accounting message. The Command Code received in the Diameter message is not an Accounting Message. A DSR Relay Agent application routing rule is mis-provisioned.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnknownCmdCodeNotify

Recovery:

1. Examine the DSR Relay Agent application routing rule for provisioning errors.

The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules**.

2. Contact the *Customer Care Center* for assistance.

22808 - Session Not Found

Event Type: CPA

Description: The CPA queried the SBR and did not get a match for a Session Binding Record based on the session id. The CPA application expected a Session Binding Record but did not find one. This condition might indicate that the SBR has timed out the record and deleted it.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterCpaSessionNotFoundNotify

Recovery:

Contact the *Customer Care Center* for assistance.

22809 - Undelivered SBR Query

Event Type: CPA

Description: The ComAgent could not deliver the SBR query or no response was received from the SBR. This event is generated when the ComAgent times out an SBR query because it could not deliver it or no response was received from the far end.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUndeliveredSbrQuery

Recovery:

1. Make sure the SBR MPs are not having networking trouble.
2. Contact the *Customer Care Center* for assistance.

22810 - Routing attempt failed due to internal resource exhaustion

Event Type: CPA

Description: An attempt to route a Diameter message through the DRL has failed due to resource exhaustion.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaRteFailResourceExhNotify

Recovery:

1. The MP may be experiencing local congestion.
2. Contact the *Customer Care Center* for assistance.

22811 - CPA Application Event Task Queue Utilization

Event Type: CPA

Description: The CPA Application's Event Queue Utilization is approaching its maximum capacity. The DSR Application's Event Queue (which processes SBR responses that are sent via ComAgent) is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: CPA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterCpaAppEventQueueUtil

Recovery:

1. The alarm log should be examined using **Main Menu** > **Alarms & Events**.

   If no additional congestion alarms are indicated, the CPA Event Task may be experiencing a problem preventing it from processing messages from its Event Queue.

2. If this problem persists, contact the *Customer Care Center* for assistance.

22812 - Missing AVP

Event Type: CPA

Description: A received Diameter Accounting message does not contain the required Accounting Record Type or Accounting Record Number AVP.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaMissingAvpNotify

Recovery:

If this problem persists, contact the *Customer Care Center* for assistance.

22813 - Received an error response to an SBR Query

Event Type: CPA

Description: CPA application received an error response in reply to an SBR query. An application specific error message was received in response to an SBR query.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 20

OID: eagleXgDiameterCpaSbrErrorRespNotify

Recovery:

If this problem persists, contact the *Customer Care Center* for assistance.

22814 - HA Sub-Resource Unavailable

Event Type: CPA

Description: An HA Sub-Resource corresponding to a partition of the Session Binding Repository is unavailable. CPA has received a callback from ComAgent indicating that an HA sub-resource is unavailable.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaHASubResourceSessionNotify

Recovery:

If this problem persists, contact the *Customer Care Center* for assistance.

22815 - Unexpected Session

Event Type: CPA

Description: A Session Binding Record was found when none was expected. CPA received an ACA-Start and found a Session Binding Record already exists.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 5

OID: eagleXgDiameterCpaUnexpectedSessionNotify

Recovery:

If this problem persists, contact the *Customer Care Center* for assistance.

22816 - One or more cSBR Subresources Unavailable

Alarm Type: CPA

Description: One or more Charging SBR Subresources are unavailable.

Severity: Based on Subresources unavailable.

- Major - one or more (but not all) cSBR Subresources are unavailable.
- Critical - all cSBR Subresources are unavailable.

Instance: Site Id

HA Score: Normal

Auto Clear Seconds: N/A

OID: eagleXgDiameterCpaSbrSubresourceIsUnavailable

Recovery:

1. Check the state of the SBR MPs.

   One or more Charging SBR subresources are unavailable. Make sure the SBR MPs are not having networking trouble.

2. Contact the *Customer Care Center* for assistance.

Tekelec Virtual Operating Environment, TVOE (24400-24499)

This section provides information and recovery procedures for the Tekelec Virtual Operation Environment (TVOE) alarms, ranging from 24400-24499.

24400 - TVOE libvirtd is down

Alarm Type: TVOE

Description: This alarm indicates that the libvirtd daemon is not running.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.1

Recovery:

If the problem persists, contact the *Customer Care Center*.

24401 - TVOE libvirtd is hung

Alarm Type: TVOE

Description: This alarm indicates that we attempted to determine if the libvirtd daemon is not responding and it didn't respond.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.2

Recovery:

If the problem persists, contact the *Customer Care Center*.

24402 - all TVOE libvirtd connections are in use

Alarm Type: TVOE

Description: This alarm indicates that all twenty connections to libvirtd are in use and more could be killed.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.31.1.1.2.3

Recovery:

If the problem persists, contact the *Customer Care Center*.

Computer Aided Policy Making, CAPM (25000-25499)

This section provides information and recovery procedures for the Computer-Aided Policy Making (CAPM) feature (i.e., Diameter Mediation) alarms and events, ranging from 25000 - 25499, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

25000 - Rule Template failed to be updated

Event Type: CAPM

Description: The Rule Template failed to update because of syntax errors. The Additional Info of the Historical alarm includes the name of the Rule Template that failed to be updated.

When the alarm is caused by CAPM Rule Template which contains a syntax error, it may not be raised immediately after applying the template, but may occur when the first Rule has been provisioned and committed.

Severity: Minor

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterCapmUpdateFailedNotify

Recovery:

1. Check the CAPM Rule Template and verify that the left-hand side term of each condition contains a valid Linking-AVP or Select expression.

   A typical problem can be a non-existing expression, or syntax error of a custom-defined Select expression. If the CAPM Rule Template contains a syntax error, create a new Rule Template by copying and modifying the existing one, then deleting the old Rule Template.

2. Verify also that the recently provisioned data of the Rule Template does not contain a syntax error, i.e., the regular expressions are correct, the fields expecting numbers contain only numbers, etc.

25001 - Action failed within the Rule Template

Event Type: CAPM

Description: When a new Rule Template is created, a failure occurs when performing the action.

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmActionFailedNotify

Recovery:

Check the reasons the action failed. It may be a lack of system resources to perform an action, or the action may refer to a part of the message that is not available.

25002 - Stop Rule Template processing after action failure

Event Type: CAPM

Description: When Action Error Handling is set to 'immediately exit from the rule template' for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped.

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmExitRuleFailedNotify

Recovery:

No action required.

25003 - Exit Trigger point after action failure

Event Type: CAPM

Description: When Action Error Handling is set to 'immediately exit from the trigger point' for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped (subsequent templates within the trigger point are also skipped).

Severity: Info

Instance: <ruleset> or <ruleset:rule-id>

HA Score: Normal

Throttle Seconds: 30

OID: eagleXgDiameterCapmExitTriggerFailedNotify

Recovery:

No action required.

OAM Alarm Management (25500-25899)

This section provides information and recovery procedures related for alarms and events related to OAM Alarm Management, ranging from 25500 - 25899, that can occur on the system. All events have a severity of Info.

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

25500 - No DA-MP Leader Detected Alarm

Alarm Type: DIAM

Description: This alarm occurs when no active DA-MP leaders have been detected.

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterNoDaMpLeaderDetectedNotify

Recovery:

If the problem persists, contact the *Customer Care Center* for assistance.

25510 - Multiple DA-MP Leader Detected Alarm

Alarm Type: DIAM

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

Severity: Critical

Instance: <NetworkElement>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterMultipleDaMpLeadersDetectedNotify

Recovery:

If the problem persists, contact the *Customer Care Center* for assistance.

Platform (31000-32700)

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

Alarms formatting information

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

The information provided about each alarm includes:

- Alarm Type: the type of alarm that has occurred. For a list of Event types see *Alarm and event types*.
- Description: describes the reason for the alarm
- Default Severity: the severity of the alarm. This severity may vary, depending on user-defined and specific application settings.
- OID: alarm identifier that appears in SNMP traps
- Alarm ID: alarm identifier that is used internally
- Recovery: provides any necessary steps for correcting or preventing the alarm

31000 - S/W fault

Alarm Type: SW

Description: Program impaired by s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrSwFaultNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact the *Customer Care Center*.

31001 - S/W status

Alarm Type: SW

Description: Program status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrSWStatusNotify

Recovery:

No action required.

31002 - Process watchdog failure

Alarm Type: SW

Description: Process watchdog timed out

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrProcWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact the *Customer Care Center*.

31003 - Tab thread watchdog failure

Alarm Type: SW

Description: Tab thread watchdog timed out

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrTabThreadWatchdogFailureNotify

Recovery:

1. Export event history for the given server and the given process.
2. Contact the *Customer Care Center*.

31100 - Database replication fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact the *Customer Care Center*.

31101 - Database replication to slave failure

Alarm Type: REPL

Description: Database replication to a slave Database has failed

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbRepToSlaveFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the *Customer Care Center*.

31102 - Database replication from master failure

Alarm Type: REPL

Description: Database replication from a master Database has failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbRepFromMasterFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the *Customer Care Center*.

31103- DB Replication update fault

Alarm Type: REPL

Description: Database replication process cannot apply update to DB

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbRepUpdateFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact the *Customer Care Center*.

31104 - DB Replication latency over threshold

Alarm Type: REPL

Description: Database replication latency has exceeded thresholds

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbRepLatencyNotify

Recovery:

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

31105 - Database merge fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbMergeFaultNotify

Recovery:

1. Export event history for the given server and inetmerge task.
2. Contact the *Customer Care Center*.

31106 - Database merge to parent failure

Alarm Type: COLL

Description: Database merging to the parent Merge Node has failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrDbMergeToParentFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the *Customer Care Center*.

31107 - Database merge from child failure

Alarm Type: COLL

Description: Database merging from a child Source Node has failed

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbMergeFromChildFailureNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the *Customer Care Center*.

31108 - Database merge latency over threshold

Alarm Type: COLL

Description: Database Merge latency has exceeded thresholds

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbMergeLatencyNotify

Recovery:

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

31109 - Topology config error

Alarm Type: DB

Description: Topology is configured incorrectly

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrTopErrorNotify

Recovery:

1. This alarm may occur during initial installation and configuration of a server. No action is necessary at that time.
2. If this alarm occurs after successful initial installation and configuration of a server, contact the *Customer Care Center*.

31110 - Database audit fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbAuditFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact the *Customer Care Center*.

31111 - Database merge audit in progress

Alarm Type: COLL

Description: Database Merge Audit between mate nodes in progress

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbMergeAuditNotify

Recovery:

No action required.

31112 - Stateful db synchronization from mate server

Alarm Type: REPL

Description: Stateful database is not yet synchronized with mate database.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 30

OID: eagleXgDsrDbRepUpLogTransTimeoutNotify

Recovery:

No action required. Contact the *Customer Care Center* if this occurs frequently.

31113 - DB replication manually disabled

Alarm Type: REPL

Description: DB Replication Manually Disabled

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrDbReplicationManuallyDisabledNotify

Recovery:

No action required.

31114 - DB replication over SOAP has failed

Alarm Type: REPL

Description: Database replication of configuration data via SOAP has failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 3600

OID: eagleXgDsrDbReplicationSoapFaultNotify

Recovery:

1. Check IMI network connectivity between the affected servers.
2. If there are no issues with network connectivity, contact the *Customer Care Center*.

31115 - Database service fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbServiceFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact the *Customer Care Center*.

31116 - Excessive shared memory

Alarm Type: MEM

Description: The amount of shared memory consumed exceeds configured thresholds

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrExcessiveSharedMemoryConsumptionNotify

Recovery:

Contact the *Customer Care Center*.

31117 - Low disk free

Alarm Type: DISK

Description: The amount of free disk is below configured thresholds

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrLowDiskFreeNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact the *Customer Care Center*.

31118 - Database disk store fault

Alarm Type: DISK

Description: Writing the database to disk failed

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbDiskStoreFaultNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, contact the *Customer Care Center*.

31119 - Database updatelog overrun

Alarm Type: DB

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbUpdateLogOverrunNotify

Recovery:

Contact the *Customer Care Center*.

31120 - Database updatelog write fault

Alarm Type: DB

Description: A Database change cannot be stored in the updatelog

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbUpdateLogWriteFaultNotify

Recovery:

Contact the *Customer Care Center*.

31121 - Low disk free early warning

Alarm Type: DISK

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrLowDiskFreeEarlyWarningNotify

Recovery:

1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
2. If there are no files known to be unneeded, contact the *Customer Care Center*.

31122 - Excessive shared memory early warning

Alarm Type: MEM

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsr

Recovery:

Contact the *Customer Care Center*.

31123 - Database replication audit command complete

Alarm Type: REPL

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

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbADICWarnNotify

Recovery:

No action required.

31124 - ADIC error

Alarm Type: REPL

Description: An ADIC detected errors

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbRepAuditCmdErrorNotify

Recovery:

Contact the *Customer Care Center*.

31125 - Database durability degraded

Alarm Type: REPL

Description: Database durability has dropped below configured durability level

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbDurabilityDegradedNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server IMI addresses.
2. If the problem persists, contact the *Customer Care Center*.

31126- Audit blocked

Alarm Type: REPL

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrAuditBlockedNotify

Recovery:

Contact the *Customer Care Center*.

31127 - DB Replication Audit Complete

Alarm Type: REPL

Description: DB replication audit completed

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbRepAuditComplete

Recovery:

No action required.

31128 - ADIC Found Error

Alarm Type: REPL

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbADICError

Recovery:

Contact the *Customer Care Center*.

31129 - ADIC Found Minor Issue

Alarm Type: REPL

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 14400

OID: eagleXgDsrDbADICWarn

Recovery:

No action required.

31130 - Network health warning

Alarm Type: NET

Description: Network health issue detected

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrNetworkHealthWarningNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server IMI addresses.

2. If the problem persists, contact the *Customer Care Center*.

31131 - IDB Throttled for Extended Period

Alarm Type: DB

Description: IDB has one or more processes throttled for an extended period.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: ThrottleWarn

Recovery:

1. Monitor for workload in excess of documented capacity.
2. Contact the *Customer Care Center* if this alarm persists.

31140 - Database perl fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbPerlFaultNotify

Recovery:

Contact the *Customer Care Center*.

31145 - Database SQL fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbSQLFaultNotify

Recovery:

1. Export event history for the given server, and Imysqld task.
2. Contact the *Customer Care Center*.

31146- DB mastership fault

Alarm Type: SW

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. Contact the *Customer Care Center*.

31147- DB upsynclog overrun

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbUpSyncLogOverrunNotify

Recovery:

Contact the *Customer Care Center*.

31148- DB lock error detected

Alarm Type: 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

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbLockErrorNotify

Recovery:

Contact the *Customer Care Center*.

31200 - Process management fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrProcMgmtFaultNotify

Recovery:

1. Export event history for the given server, all processes.
2. Contact the *Customer Care Center*.

31201 - Process not running

Alarm Type: PROC

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrProcNotRunningNotify

Recovery:

Contact the *Customer Care Center*.

31202 - Unkillable zombie process

Alarm Type: PROC

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrProcZombieProcess

Recovery:

1. If the process does not exit, it may be necessary to reboot the server to eliminate the zombie process.
2. Contact the *Customer Care Center*.

31206 - Process mgmt monitoring fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrProcMgmtMonFaultNotify

Recovery:

Contact the *Customer Care Center*.

31207 - Process resource monitoring fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrProcResourceMonFaultNotify

Recovery:

Contact the *Customer Care Center*.

31208 - IP port server fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrPortServerFaultNotify

Recovery:

Contact the *Customer Care Center*.

31209 - Hostname lookup failed

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHostLookupFailedNotify

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, contact the *Customer Care Center*.

31213 - Process scheduler fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrProcSchedulerFaultNotify

Recovery:

Contact the *Customer Care Center*.

31214 - Scheduled process fault

Alarm Type: PROC

Description: A scheduled process cannot be executed or abnormally terminated

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrScheduleProcessFaultNotify

Recovery:

Contact the *Customer Care Center*.

31215 - Process resources exceeded

Alarm Type: SW

Description: A process is consuming excessive system resources

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 14400

OID: eagleXgDsrProcResourcesExceededFaultNotify

Recovery:

Contact the *Customer Care Center*.

31216 - SysMetric configuration error

Alarm Type: SW

Description: A SysMetric Configuration table contains invalid data

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrSysMetricConfigErrorNotify

Recovery:

Contact the *Customer Care Center*.

31220 - HA configuration monitor fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaCfgMonitorFaultNotify

Recovery:

Contact the *Customer Care Center*.

31221 - HA alarm monitor fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaAlarmMonitorFaultNotify

Recovery:

Contact the *Customer Care Center*.

31222 - HA not configured

Alarm Type: HA

Description: High availability is disabled due to system configuration

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaNotConfiguredNotify

Recovery:

Contact the *Customer Care Center*.

31223 - HA Heartbeat transmit failure

Alarm Type: HA

Description: The high availability monitor failed to send heartbeat

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaHbTransmitFailureNotify

Recovery:

1. This alarm clears automatically when the server successfully registers for HA heartbeating.
2. If this alarm does not clear after a couple minutes, contact the *Customer Care Center*.

31224 - HA configuration error

Alarm Type: HA

Description: High availability configuration error

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaCfgErrorNotify

Recovery:

Contact the *Customer Care Center*.

31225 - HA service start failure

Alarm Type: HA

Description: The high availability service failed to start

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaSvcStartFailureNotify

Recovery:

1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, contact the *Customer Care Center*.

31226 - HA availability status degraded

Alarm Type: HA

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact the *Customer Care Center*.

31227 - HA availability status failed

Alarm Type: HA

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

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaAvailFailedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, contact the *Customer Care Center*.

31228 - HA standby offline

Alarm Type: HA

Description: High availability standby server is offline

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrHaStandbyOfflineNotify

Recovery:

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

31229 - HA score changed

Alarm Type: HA

Description: High availability health score changed

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaScoreChangeNotify

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrRecAlarmEvProcFaultNotify

Recovery:

1. Export event history for the given server and raclerk task.
2. Contact the *Customer Care Center*.

31231 - Platform alarm agent fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrPlatAlarmAgentNotify

Recovery:

Contact the *Customer Care Center*.

31232- Late heartbeat warning

Alarm Type: HA

Description: High availability server has not received a heartbeat within the configured interval. High availability server has not received a message on specified path within the configured interval.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaLateHeartbeatWarningNotify

Recovery:

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

31233 - HA Secondary Path DownHA Path Down

Alarm Type: HA

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaSecPathDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the secondary path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.

2. If communication fails at any other time, look for network connectivity issues on the secondary network.
3. Contact the *Customer Care Center*.

31234 - Untrusted Time Upon Initialization

Alarm Type: 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:

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrUtrustedTimeOnInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, contact the *Customer Care Center*.

31235 - Untrusted Time After Initialization

Alarm Type: REPL

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

Severity: Critical

Instance:

HA Score: Normal

Auto Clear Seconds: 0

OID: eagleXgDsrUntrustedTimePostOnInit

Recovery:

1. Correct NTP configuration.
2. If the problem persists, contact the *Customer Care Center*.

31240 - Measurements collection fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrMeasCollectorFaultNotify

Recovery:

1. Export event history for the given server and statclerk task.
2. Contact the *Customer Care Center*.

31250 - RE port mapping fault

Alarm Type: SW

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrRePortMappingFaultNotify

Recovery:

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

31260 - Database SNMP Agent

Alarm Type: SW

Description: The Database SNMP agent (snmpIdbAgentcmsnmpa) is impaired by a s/w fault

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrDbcomcolSnmpAgentNotify

Recovery:

1. Export event history for the given server and all processes.
2. Contact the *Customer Care Center*.

31270 - Logging output

Alarm Type: SW

Description: Logging output set to Above Normal

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrLoggingOutputNotify

Recovery:

Extra diagnostic logs are being collected, potentially degrading system performance. Contact the *Customer Care Center*.

31280 - HA Active to Standby transition

Alarm Type: HA

Description: HA active to standby activity transition

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31281 - HA Standby to Active transition

Alarm Type: HA

Description: HA standby to active activity transition

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrStandbyToActiveTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31282- HA Management Fault

Alarm Type: HA

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaMgmtFaultNotify

Recovery:

Export event history for the given server and cmha task, then Contact the *Customer Care Center*.

31283- HA Server Offline

Alarm Type: HA

Description: High availability server is offline

Severity: Critical

HA Score: Normal

Auto Clear Seconds: 0

OID: eagleXgDsrHAServerOfflineNotify

Recovery

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

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Type: HA

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaRemoteHeartbeatWarningNotify

Recovery:

1. No action required. This is a warning and can be due to transient conditions. The remote subscriber will move to another server in the cluster.
2. If there continues to be no heartbeat from the server, contact the *Customer Care Center*.

31290- HA Process Status

Alarm Type: HA

Description: HA manager (cmha) status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaProcessStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31291- HA Election Status

Alarm Type: HA

Description: HA DC Election status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHAElectionStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31292- HA Policy Status

Alarm Type: HA

Description: HA Policy plan status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaPolicyStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31293- HA Resource Link Status

Alarm Type: HA

Description: HA ResourceAgent Link status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaRaLinkStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31294- HA Resource Status

Alarm Type: HA

Description: HA Resource registration status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaResourceStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31295- HA Action Status

Alarm Type: HA

Description: HA Resource action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaActionStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31296- HA Monitor Status

Alarm Type: HA

Description: HA Monitor action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaMonitorStatusNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31297- HA Resource Agent Info

Alarm Type: HA

Description: HA Resource Agent Info

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaRaInfoNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31298- HA Resource Agent Detail

Alarm Type: HA

Description: Resource Agent application detailed information

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaRaDetailNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, contact the *Customer Care Center*.

31299 - HA Notification Status

Alarm Type: HA

Description: HA Notification status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaNotification

Recovery:

No action required.

31300 - HA Control Status

Alarm Type: HA

Description: HA Control action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: eagleXgDsrHaControl

Recovery:

No action required.

32113 - Uncorrectable ECC memory error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.1.14

Recovery

Contact the *Customer Care Center* to request hardware replacement.

32114 - SNMP get failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.1.15

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

Recovery

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

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Type: TPD

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.1.16

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. If the problem persists, contact the *Customer Care Center*.

32116 - TPD Server's Time Has Gone Backwards

Alarm Type: TPD

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.1.17

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. If the problem persists, contact the *Customer Care Center*.

32117 - TPD NTP Offset Check Failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.1.18

Recovery:

1. Run syscheck in verbose mode.
2. Contact the *Customer Care Center*.

32300 – Server fan failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.1

Recovery

Contact the *Customer Care Center*.

32301 - Server internal disk error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.2

Recovery

Contact the *Customer Care Center*.

32302 – Server RAID disk error

Alarm Type: TPD

Description: This alarm indicates that the offboard storage server had a problem with its hardware disks.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.3

Recovery

Contact the *Customer Care Center*.

32303 - Server Platform error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.4

Recovery

Contact the *Customer Care Center* and provide the system health check output.

32304 - Server file system error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.5

Recovery

Contact the *Customer Care Center*.

32305 - Server Platform process error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.6

Recovery

Contact the *Customer Care Center*.

32307 - Server swap space shortage failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.8

Recovery

Contact the *Customer Care Center*.

32308 - Server provisioning network error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.9

Recovery

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

32312 - Server disk space shortage error

Alarm Type: TPD

Description: This alarm indicates that one of the following conditions has occurred:

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.13

Recovery

Contact the *Customer Care Center*.

32313 - Server default route network error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.14

Recovery

Contact the *Customer Care Center*.

32314 - Server temperature error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.15

Recovery

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

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

3. If the problem has not been resolved, contact the *Customer Care Center*.

32315 – Server mainboard voltage error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.16

Recovery

Contact the *Customer Care Center*.

32316 – Server power feed error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.17

Recovery

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

6. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
7. If the problem has not been resolved, contact the *Customer Care Center*.

32317 - Server disk health test error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.18

Recovery

1. Perform the recovery procedures for the other alarms that accompany this alarm.
2. If the problem has not been resolved, contact the *Customer Care Center*.

32318 - Server disk unavailable error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.19

Recovery

Contact the *Customer Care Center*.

32319 – Device error

Alarm Type: TPD

This alarm indicates that the offboard storage server had a problem with its disk volume filling up.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.20

Recovery

Contact the *Customer Care Center*.

32320 – Device interface error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.21

Recovery

Contact the *Customer Care Center*.

32321 – Correctable ECC memory error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.22

Recovery

No recovery necessary. If the condition persists, contact the *Customer Care Center* to request hardware replacement.

32322 – Power Supply A error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.23

Recovery

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact the *Customer Care Center*.

32323 – Power Supply B error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.24

Recovery

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. If the problem persists, contact the *Customer Care Center*.

32324 – Breaker panel feed error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.25

Recovery

1. Verify that the same alarm is displayed by multiple servers:

- If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
- If this alarm is displayed by multiple servers, go to the next step.

2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.
3. If the problem has not been resolved, contact the *Customer Care Center* to request that the breaker panel be replaced.

32325 – Breaker panel breaker error

Alarm Type: TPD

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 4: Breaker Panel LEDs*) identify whether the fault occurred on the input power or the output power, as follows:

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

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

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

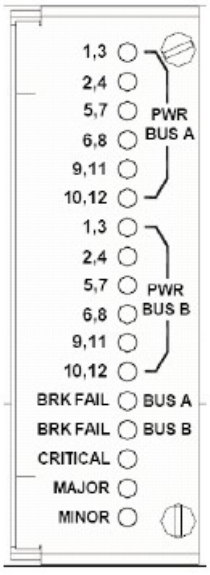


Figure 4: Breaker Panel LEDs

Description: This alarm indicates that a power fault has been identified by the breaker panel.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.26

Recovery

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

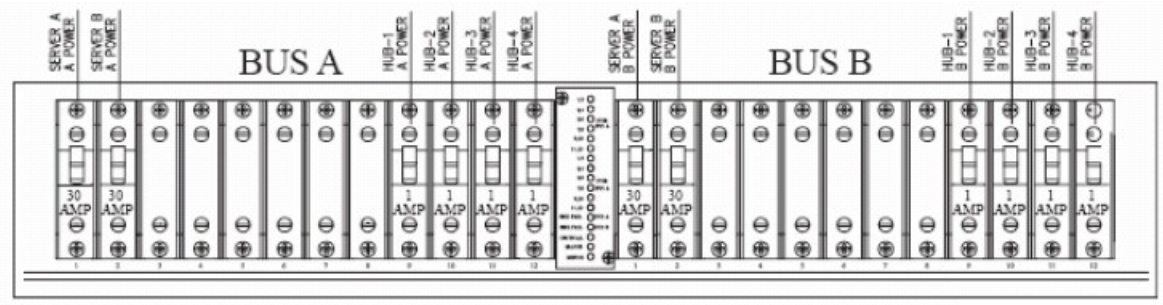


Figure 5: Breaker Panel Setting

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. Contact the *Customer Care Center*

a) 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.
b) Check the LEDs in the PWR BUS A group and the PWR BUS B group again.
   - If the LEDs are now illuminated Green, the issue has been resolved.
   - Proceed to *Substep c* to verify that the alarm has been cleared.
   - If the LEDs are still illuminated Red, continue to the next sub-step.
c) 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.

d) 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.

- If the LEDs are now illuminated Green, the issue has been resolved. Proceed to *Step 3* to verify that the alarm has been cleared.
- If the LEDs are still illuminated Red, skip to *Step 4*

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

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

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

b) After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, Contact the *Customer Care Center*

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

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 problem has not been resolved, contact the *Customer Care Center*

32326 – Breaker panel monitoring error

Alarm Type: TPD

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 or
- 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: 1.3.6.1.4.1.323.5.3.18.3.1.2.27

Recovery

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

32327 – Server HA Keepalive error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.28

Recovery

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

   Note: This step may require command line ability.

4. Contact the *Customer Care Center*.

32331 – HP disk problem

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.32

Recovery

Contact the *Customer Care Center*.

32332 – HP Smart Array controller problem

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.33

Recovery

Contact the *Customer Care Center*.

32333 – HP hpacucliStatus utility problem

Alarm Type: TPD

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 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: 1.3.6.1.4.1.323.5.3.18.3.1.2.34

Recovery

Contact the *Customer Care Center*.

32334 - Multipath device access link problem

Alarm Type: TPD

Description: One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.35

Recovery

32335 - Switch link down error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.36

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

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

Recovery

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, contact the *Customer Care Center* who should verify port settings on both the server and the switch.

32336– Half Open Socket Limit

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.37

Recovery

Contact the *Customer Care Center*.

32337 - E5-APP-B Firmware Flash

Alarm Type: TPD

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

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.38

Recovery:

Contact the *Customer Care Center*.

32338 - E5-APP-B Serial mezzanine seating

Alarm Type: TPD

Description: This alarm indicates the serial mezzanine board was not properly seated.

Severity: Major

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.39

Recovery:

Contact the *Customer Care Center*.

32339 - Max pid limit

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.40

Recovery:

1. Run syscheck in verbose mode.
2. Contact the *Customer Care Center*.

32340 - Server NTP Daemon Lost Synchronization

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.41

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. Contact the *Customer Care Center*.

32341 - Server NTP Daemon Never Synchronized Error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.42

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. Contact the *Customer Care Center*.

32342 - NTP Offset Check Error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.43

Recovery:

1. Verify NTP settings and that NTP are providing accurate time.
2. Contact the *Customer Care Center*.

32343 - RAID disk problem

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.44

Recovery:

1. Run syscheck in verbose mode.
2. Contact the *Customer Care Center*.

32344 - RAID controller problem

Alarm Type: TPD

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.2.45

Recovery:

1. Run syscheck in verbose mode.
2. Contact the *Customer Care Center*.

32345 - Server Upgrade snapshot(s) invalid

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.2.46

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. Contact the *Customer Care Center*

32500 – Server disk space shortage warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.1

Recovery

Contact the *Customer Care Center*.

32501 – Server application process error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.2

Recovery

Contact the *Customer Care Center*.

32502 – Server hardware configuration error

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.3

Recovery

Contact the *Customer Care Center*.

32503 – Server RAM shortage warning

Alarm Type: TPD

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.4

Recovery

Contact the *Customer Care Center*.

32505 – Server swap space shortage warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.6

Recovery

Contact the *Customer Care Center*.

32506 – Server default router not defined

Alarm Type: TPD

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.7

Recovery

Contact the *Customer Care Center*.

32507 – Server temperature warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.8

Recovery

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

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

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

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

4. If the problem has not been resolved, contact the *Customer Care Center*.

32508 – Server core file detected

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.9

Recovery

32509 – Server NTP Daemon not synchronized

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.10

Recovery

Contact the *Customer Care Center*.

32510 – CMOS battery voltage low

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.11

Recovery

Contact the *Customer Care Center*.

32511 – Server disk self test warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.12

Recovery

Contact the *Customer Care Center*.

32512 – Device warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.13

Recovery

Contact the *Customer Care Center*.

32513 – Device interface warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.14

Recovery

Contact the *Customer Care Center*.

32514 – Server reboot watchdog initiated

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.15

Recovery

Contact the *Customer Care Center*.

32515 – Server HA failover inhibited

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.16

Recovery

Contact the *Customer Care Center*.

32516 – Server HA Active to Standby transition

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.17

Recovery

Contact the *Customer Care Center*.

32517 – Server HA Standby to Active transition

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.18

Recovery

Contact the *Customer Care Center*.

32518 – Platform Health Check failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.19

Recovery

Contact the *Customer Care Center*.

32519 – NTP Offset Check failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.20

Recovery

Contact the *Customer Care Center*.

32520 – NTP Stratum Check failure

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.21

Recovery

Contact the *Customer Care Center*.

32521 – SAS Presence Sensor Missing

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.22

Recovery

Contact the *Customer Care Center* to get a replacement server.

32522 – SAS Drive Missing

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.23

Recovery

Contact the *Customer Care Center* to determine whether the issue is with a failed drive or failed configuration.

32523 – DRBD failover busy

Alarm Type: TPD

Description: This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.4.1.323.5.3.18.3.1.3.24

Recovery

A DRBD sync should not take more than 15 minutes to complete. Please wait for approximately 20 minutes, and then check if the DRBD sync has completed. If the alarm persists longer than this time period, contact the *Customer Care Center*.

32524 – HP disk resync

Alarm Type: TPD

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 dependant 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: 1.3.6.1.4.1.323.5.3.18.3.1.3.25

Recovery

Contact the *Customer Care Center*.

32525 – Telco Fan Warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.26

Recovery

1. Contact the *Customer Care Center* to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.
2. *Customer Care Center* personnel can perform an snmpget command or log into the switch to get detailed fan status information.

32526 – Telco Temperature Warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.27

Recovery

1. Lower the ambient air temperature around the switch as low as possible.
2. If problem persists, contact the *Customer Care Center*.

32527 – Telco Power Supply Warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.28

Recovery

1. Verify breaker wasn't tripped.
2. If breaker is still good and problem persists, contact the *Customer Care Center* who can perform a **snmpget** command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 – Invalid BIOS value

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.29

Recovery

Contact the *Customer Care Center*.

32529– Server Kernel Dump File Detected

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.30

Recovery

Contact the *Customer Care Center*.

32530– Server Upgrade Fail Detected

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.31

Recovery

Contact the *Customer Care Center*.

32531– Half Open Socket Warning

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.32

Recovery

Contact the *Customer Care Center*.

32532– Server Upgrade Pending Accept/Reject

Alarm Type: TPD

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: 1.3.6.1.4.1.323.5.3.18.3.1.3.33

Recovery

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

32533 - Max pid warning

Alarm Type: TPD

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: 1.3.6.1.2.1.323.5.3.18.3.1.3.34

Recovery:

1. Run syscheck in verbose mode.
2. Contact the *Customer Care Center*.

32534 - NTP Source Server Is Not Able To Provide Correct Time

Alarm Type: TPD

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: 1.3.6.1.2.1.323.5.3.18.3.1.3.35

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. Contact the *Customer Care Center*.

32535 - RAID disk resync

Alarm Type: TPD

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 dependant on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: 1.3.6.1.2.1.323.5.3.18.3.1.3.36

Recovery:

1. Run syscheck in verbose mode
2. If this alarm persists for several hours (depending on a load of a server rebuild of array can take multiple hours to finish), contact the *Customer Care Center*.

32536 - Server Upgrade snapshot(s) warning

Alarm Type: TPD

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: 1.3.6.1.2.1.323.5.3.18.3.1.3.37

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. Contact the *Customer Care Center*

GLA (33100-33149)

This section provides information and recovery procedures for GLA alarms and events, ranging from 33100 to 33149, and lists the type of alarms and events that can occur on the system.

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

33100 - GLA Message Decoding Failure

Event Group: GLA

Description: Message received was rejected because of a decoding failure

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaMessageDecodingFailure

Recovery:

1. While parsing the message, one of the following conditions occurred:
   - The message content was inconsistent with the "Message Length" in the message header.
   - The IMSI contained in the User-Name AVP was considered invalid due to length.
   - The MSISDN contained in the MSISDN AVP was considered invalid due to length.
2. These protocol errors can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node. Collect a trace containing the GGR, and determine which node is causing the invalid data.
3. If the problem persists, contact the *Customer Care Center*.

33101 - GLA Incorrect Application ID or Command Code

Event Group: GLA

Description: Message received was rejected because the Application ID was not GL (16777321) or the Command Code was not GGR (8388655).

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaIncorrectApplIdOrCmdCodeNotify

Recovery:

Examine the Application Routing Rules that direct traffic to GLA and verify that the Application ID is set to GL (16777321) and the Command Code is set to GGR (8388655) for all Application Routing Rules referring to GLA.

33102 - GLA Missing Subscriber ID

Event Group: GLA

Description: Message received was rejected because it did not contain and IMSI or an MSISDN in a Subscription-ID AVP

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaMissingSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.

2. If this condition is met, inspect each element between the GQC and GWS to determine if Subscriber information within the Request is being modified.

33103 - GLA Communication Agent Error

Event Group: GLA

Description: GLA was unable to communicate with the pSBR-Binding due to a communications error

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaComAgentErrorNotify

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. Examine the status of the Reporting Server's BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persist, contact the *Customer Care Center*.

33104 - GLA Duplicate Subscriber ID

Event Group: GLA

Description: Message received was rejected because it contained both a User-Name AVP and a MSISDN AVP

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaDuplicateSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.
2. Inspect each element between teh GQC and GQS to determine which node is inserting bot AVPs and correct that node so that only one AVP is included in the GGR.

33105 - Routing Attempt failed due to queue exhaustion

Event Group: GLA

Description: Message could not be routed because the internal "Answer Message Queue" to the DSR Relay Agent was full.

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaRoutingAttemptFailureDrlQueueExhNotify

Recovery:

1. This condition should not occur unless the DSR is experiencing severe congestion due to excessive traffic levels arriving on the DRL Answer Queue.
2. GL traffic should be diverted from the DA-MP to other DA-MPs in the DSR, or to another DSR.

33106 - GLA Communication Agent Timeout

Event Group: GLA

Description: GLA was unable to communicate with the pSBR-Binding and the query timed out.

Severity: Info

Instance: "MP"

HA Score: Normal

Throttle Seconds: 60

OID: eagleXgDiameterGlaComAgentTimeoutNotify

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. Examine the status of the Reporting Server's BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, contact the *Customer Care Center*.

33120 - Policy SBR Binding Sub-Resource Unavailable

Alarm Group: GLA

Description: GLA is unable to communicate with Policy SBR-Binding. One or more binding sub-resources are unavailable.

Severity:

- **Major:** When at least one server group that has a range of binding sub-resources is not available, but at least the minimum number of binding sub-resources is still available.
- **Critical:** When fewer than the minimum number of binding sub-resources are not available.

Instance: GLA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterGlaBindingSubresourceUnavailableNotify

Recovery

1. Monitor the Policy DRA Binding Resource on the GLA NO at **Main Menu** > **Configuration** > **Resource Domains**.
2. Determine if some of the pSBR-B MPs are unavailable or out-of-service. In this case, all DA-MPs and all pSBR-B MPs will also report ComAgent connection alarms.
3. Determine if there is a WAN outage. In this case, DA-MPs should also report ComAgent connection alarms to remote pSBR-Bs, and local pSBR-Bs should report ComAgent connection alarms to remote DA-MPs.
4. Determine if there is a network routing issue. In this case, one or a few DA-MPs may report a ComAgent connection against a limited number of pSBR-Bs.
5. If the problem persists, contact the *Customer Care Center* for assistance.

33121 - GLA pSBR-B Response Task Message Queue Utilization

Alarm Group: GLA

Description: GLA's pSBR-B Response Message Queue Utilization is approaching its maximum capacity.

Severity: Minor, Major, Critical

Instance: RxGlaResponseMsgQueue, GLA

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDiameterGlaBindingSubresourceUnavailableNotify

Recovery

1. Determine if the GLA pSBR Response Task is mis-configured (Eg. Smaller response task queue size / fewer number of response task threads as compared to the request task threads).
2. Determine if the GLA pSBR Response Task has encountered a problem preventing it from processing messages from its Task Message Queue even if no additional congestion alarms are asserted.
3. If the problem persists, contact the *Customer Care Center* for additional assistance.

Chapter 4

Key Performance Indicators (KPIs)

Topics:

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

General KPIs information

This section provides general information about KPIs, the Status and Manage KPI page, and how to view KPIs.

KPIs overview

Key Performance Indicators (KPIs) allow the user to monitor system performance data, including CPU, memory, swap space, and uptime per server. This performance data is collected from all servers within the defined topology.

The KPI display function resides on all OAM servers. Servers that provide a GUI connection rely on KPI information merged to that server. The Network OAMP servers maintain status information for all servers in the topology. System OAM servers have reliable information only for servers within the same network element.

The Status and Manage KPIs page displays performance data for the entire system. KPI data for the entire system is updated every 60 seconds. If data is not currently being collected for a particular server, the KPI for that server will be shown as Unk for "Unknown".

KPIs

The **Status & Manage > KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server.

KPIs server elements

Table 11: KPIs Server Elements

KPIs Status Element	Description
Name	The KPI name.
Max	Maximum value of the KPI name within the selected scope.
Min	Minimum value of the KPI name within the selected scope.
Median	Median value of the KPI name within the selected scope.
Average	Average value of the KPI name within the selected scope.
Sum	Summary of all values of the KPI name within the selected scope.
Description	Description of the KPI name.

Viewing KPIs

Use this procedure to view KPI data.

1. Select **Status & Manage > KPIs**.

   The **Status & Manage KPIs** page appears with the **Server** tab displayed. For details about the KPIs displayed on this page, see the application documentation.

2. Click to select an application tab to see KPI data relevant to the application.

   Note: The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server. Collection of KPI data is handled solely by NOAMP servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the **KPIs Export** page.

Table 12: Schedule KPI Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments

Element	Description	Data Input Notes
		Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting KPIs

You can schedule periodic exports of security log data from the **KPIs** page. KPI data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the **KPIs** page, only filtered data is exported.

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

Use this procedure to schedule a data export task.

1. Select **Status & Manage > KPIs**.

   The **KPIs** page appears.

2. If necessary, specify filter criteria and click **Go**.
   The KPIs are displayed according to the specified criteria.
3. Click **Export**.
   The **Schedule KPI Data Export** page appears.
4. Enter the **Task Name**.
   For more information about **Task Name**, or any field on this page, see *KPIs data export elements* .
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the **Minutes.**
7. Select the **Time of Day**.

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

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

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

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

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

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

   - *Viewing scheduled tasks*
   - *Editing a scheduled task*

- *Deleting a scheduled task*
- *Generating a scheduled task report*

Computer Aided Policy Making (CAPM) KPIs

The KPI values associated with CAPM are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 13: CAPM KPIs

Variable	Description
Processing time [ms]	Average processing time of Rule Template on a per Rule Template basis.
Active Templates	Number of Rule Templates that are in Active state.
Test Templates	Number of Rule Templates that are in Test state.
Development Templates	Number of Rule Templates that are in Development state.

Charging Proxy Application (CPA) KPIs

The KPI values associated with CPA are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Table 14: Charging Proxy Application (CPA) KPIs

Variable	Description
CPA Answer Message Rate	Track the average number of Answer messages processed per second by the CPA application.
CPA Ingress Message Rate	Track the average number of Diameter messages received per second by the CPA application.
CPA Request Message Rate	Track the average number of Request messages processed per second by the CPA application.
cSBR Query Error Rate	Track the average number of errors received per second by the CPA application when attempting to query (read, create, update, delete) SBR.
cSBR Query Rate	Track the average number of SBR Queries sent per second by the CPA application.

Communication Agent (ComAgent) KPIs

The KPI values associated with ComAgent are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 15: Communication Agent KPIs

Variable	Description
User Data Ingress message rate	Average of User Data Ingress Message Rate (messages per second) utilization on a MP server. The Ingress Message Rate is the number of User Data StackEvents (messages) that ComAgent delivers to Application Layers Queue.

Connection Maintenance KPIs

The KPI values associated with Connection Maintenance are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 16: 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 17: DIAM KPIs

Variable	Description
Ingress Trans Success Rate	Percentage of ingress peer-to-peer transactions successfully complete
Avg Rsp Time	Average time from when routing receives a Request message from a downstream peer to the time that an Answer response is sent to that downstream peer

Variable	Description
Routing Success Rate	Percentage of transactions successfully routed on first attempt
Avg Diameter Process CPU Util	Average percent Diameter process CPU utilization (0-100%) on an MP server
Avg IMR Offered	Average Ingress Offered message rate (messages per second) on a MP server . Offered message rate is number of ingress Diameter messages before any Ingress controls are applied
Avg IMR Accepted	Average Ingress Accepted message rate (messages per second) on a MP server. Accepted message rate is number of routable messages accepted by MP after all Ingress controls are applied
Avg Message Processing Load	Average message processing load (messages per second) on a MP server. The message processing load is the number of Diameter messages that are routed , including Reroutes and Msgcopy

GLA KPIs

The KPI values associated with GLA are visible using **Main Menu** > **Status & Manage** > **KPIs**

Variable	Description
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on an MP server for this DSR Application. The Ingress Message Rate is the number of ingress Diameter messages that are selected for processing by the ART and sent to the DSR Application for processing.
Success Message Rate	GLA Success Message Rate (messages per second) on an MP server. The Success Message Rate is the number of ingress Diameter messages that are processed by GLA and answered with a success (2xxx) result code).

IDIH KPIs

The KPI values associated with the IDIH will be visible via the GUI **Main Menu** > **Status & Manage** > **KPIs**

Variable	Description
DSR-DIH TTR Bandwidth	Average bandwidth used by DSR in sending TTRs, (including trace start and stop messages), to DIH, in megabytes per second.

IP Front End (IPFE) KPIs

The KPI values associated with IPFE are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Table 18: IPFE KPIs

Variable	Description
CPU %	Total CPU used by the IPFE process
Memory Total	Absolute memory used by the IPFE process
Memory %	Percent memory used by the IPFE process
Mem. Heap	Total heap allocated by the IPFE process
IPFE Packets/Sec	The average number of packets per second the IPFE receives
IPFE MBytes/Sec	The average number of megabytes per second the IPFE receives

Message Processor (MP) KPIs

The KPI values associated with MP are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 19: MP KPIs

Variable	Description
Avg Diameter Process CPU Util	Average percent Diameter Process CPU utilization (0-100%) on a MP server.
Avg IMR Offered	Average Ingress Offered message rate (messages per second) on a MP server . Offered message rate is number of ingress Diameter messages before any Ingress controls are applied.
Avg IMR Accepted	Average Ingress Accepted message rate (messages per second) on a MP server . Accepted message rate is number of routable messages accepted by MP after all Ingress controls are applied.

Variable	Description
Avg Messsage Processing Load	Average message processing load (messages per second) on a MP server. The message processing load is the number of Diameter messages that are routed , including Reroutes and Msgcop.

Full Address Based Resolution (FABR) KPIs

The KPI values associated with FABRr are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 20: FABR KPIs

Variable	Description
Ingress Message Rate	Ingress Message Rate (messages per second) utilization on a MP server for the FABR Application. The Ingress Message Rate is the number of ingress Diameter messages that were successfully received by the FABR Application.
Resolved Message Rate	Resolved Message Rate (messages per second) utilization on a MP server. The Resolved Message Rate is the number of ingress Diameter messages that are successfully resolved to a Destination by the FABR application.
DP Response Time Average	Average DP response time is the average time (in milliseconds) it takes to receive a DP response after sending the corresponding DP query.

Policy Diameter Routing Agent (PDRA) KPIs

The KPI values associated with PDRA are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 21: P-DRA KPIs

Variable	Description
P-DRA Ingress Message Rate	This KPI is to measure the average number of Diameter messages per second including both requests and answers received by P-DRA from the DRL layer.

Policy SBR (pSBR) KPIs

The KPI values for pSBR are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Table 22: pSBR KPIs

Variable	Description
pSBR memory utilization (0-100%)	This KPI helps monitoring of the pSBR memory utilization
pSBR process CPU utilization (0-100%)	This KPI helps monitoring of the pSBR process CPU utilization

Table 23: pSBR-Binding KPIs

Variable	Description
Total number of subscribers with at least one binding	This KPI provides usage information about the current number of subscribers (distinct IMSI values) that have at least one binding.
Average number of binding DB reads per second	This KPI helps monitoring of the binding DB performance.
Average number of binding DB writes per second	This KPI helps monitoring of the binding DB performance.

Note: In order to view the current number of subscribers with a binding for the entire P-DRA network, an appropriate scope must be chosen on the KPI screen. Valid scopes must encompass all binding pSBR servers as follows: Entire Network, filtered by Resource Domain with the Policy Binding resource domain selected, or filtered by Place Association with the Policy DRA Binding Region place association selected.

Table 24: pSBR-Session KPIs

Variable	Description
Total Number of Active Sessions	This KPI displays the total number of sessions running on the pSBR network to facilitate performance monitoring and capacity planning.
Average number of session DB reads per second	This KPI helps monitoring of the binding DB performance.
Average number of session DB writes per second	This KPI helps monitoring of the binding DB performance.

Range Based Address Resolution (RBAR) KPIs

The KPI values associated with RBAR are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 25: RBAR KPIs

Variable	Description
Avg Resolved Message Rate	Average Resolved Message Rate (messages per second) utilization on a MP server. The Resolved Message Rate is the number of ingress Diameter messages that are successfully resolved to a Destination by the Range Based Address Resolution application.
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on a MP server for this DSR Application. The Ingress Message Rate is the number of ingress Diameter messages that were successfully received by the DSR Application.

Session Binding Repository (SBR) KPIs

The KPI values associated with SBR are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Table 26: SBR KPIs

Variable	Description
Current session bindings	Current number of session bindings
Mostly Stale session bindings	Number of session bindings found to be Mostly Stale during the previous audit
Session binding capacity	Number of session bindings as a percentage of the total capacity
Load Shed Rate	Rate (per second) at which queries (read, create, update, delete) are being shed due to congestion
Time to process query	Lifetime of a transaction in microseconds (time between query received and response sent)
Query rate	Number of queries (read, create, update, delete) processed per second

Chapter 5

Measurements

Topics:

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

General measurements information

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

Measurements

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

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

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

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

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

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

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

Measurement elements

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

Table 27: Measurements Elements

Element	Description	Data Input Notes
Scope	Network Elements, Server Groups, Resource Domains, Places and Place Associations for which the measurements report can be run. **Note:** Measurements for SOAM network elements are not available in systems that do not support SOAMs.	Format: Pulldown list Range: Network Elements in the topology; Server Groups in the topology; Resource Domains in the topology; Places in the topology; Place Associations in the topology **Note:** If no selection is made, the default scope is Entire Network. Default: Entire Network
Report	A selection of reports	Format: Pulldown list Range: Varies depending on application Default: Group
Column Filter	The characteristics for filtering the column display	Format: Pulldown list Range: Sub-measurement Sub-measurement Ranges: • Like: A pattern-matching distinction for sub-measurement name, for example, 123* matches any sub-measurement that begins with 123. • In: A list-matching distinction for sub-measurement ID, for example, 3,4,6-10 matches only sub-measurements 3, 4, and 6 through 10. Default: None
Time Range	The interval of time for which the data is being reported, beginning or ending on a specified date.	Format: Pulldown list Range: Days, Hours, Minutes, Seconds Interval Reference Point: Ending, Beginning Default: Days

Generating a measurements report

Use this procedure to generate and view a measurements report.

1. Select **Measurements > Report**.

   The **Measurements Report** page appears.

2. Select the **Scope**.

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

3. Select the **Report**.
4. Select the **Interval**.
5. Select the **Time Range**.
6. Select **Beginning** or **Ending** as the **Time Range** interval reference point.
7. Select the **Beginning** or **Ending** date.
8. Click **Go**.

   The report is generated.

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

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

   The report data appears.

Measurements data export elements

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

Table 28: Schedule Measurement Data Export Elements

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

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

Exporting measurements reports

You can schedule periodic exports of data from the **Measurements Report** page. Measurements data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied on the **Measurements Report** page, only filtered data is exported.

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

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

1. Select **Measurements > Report**.

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

2. Generate a measurements report.

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

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

   The measurement report is exported to a CSV file. Click the link at the top of the page to go directly to the **Status & Manage** > **Files** page. From the **Status & Manage** page, you can view a list of files

available for download, including the measurements report you exported during this procedure. The **Schedule Measurement Log Data Export** page appears.

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

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

6. Select the **Export Frequency**.

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

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

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

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

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

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

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

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

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

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

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

Address Resolution Exception measurements

The Address Resolution Exception measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the RBAR Application.

Table 29: Address Resolution Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxRbarDecodeFailureResol	Number of Request messages rejected due to a message decoding error.	5 min

Measurement Tag	Description	Collection Interval
RxRbarInvalidImsiMcc	Number of times an AVP instance present in Diameter request message is rejected due to the MCC contained in the decoded IMSI falls within one of the configured Reserved MCC Ranges	5 min
RxRbarResolFailAll	Number of Request messages received which did not resolve to a provisioned address or address range.	5 min
RxRbarResolFailCmdcode	Number of Request messages received with an unknown Command Code.	5 min
RxRbarResolFailDbFail	Number of routing attempt failures due to internal database inconsistency failure.	5 min
RxRbarResolFailImpiMatch	Number of Request messages received with a valid IMPI that did not match a provisioned address or address range.	5 min
RxRbarResolFailImpuMatch	Number of Request messages received with a valid IMPU that did not match a provisioned address or address range.	5 min
RxRbarResolFailImsiMatch	Number of Request messages received with a valid IMSI that did not match a provisioned address or address range.	5 min
RxRbarResolFailIpv4Match	Number of Request messages received with an IPv4 Address that did not match a provisioned address or address range.	5 min
RxRbarResolFailIpv6prefixMatch	Number of Request messages received with an IPv6-Prefix Address that did not match a provisioned address or address range.	5 min
RxRbarResolFailMsisdnMatch	Number of Request messages received with a valid MSISDN that did not match a provisioned address or address range.	5 min
RxRbarResolFailNoAddrAvps	Number of Request messages received without a Routing Entity Address AVP.	5 min
RxRbarResolFailNoValidAddr	Number of Request messages received with at least Routing Entity Address	5 min

Measurement Tag	Description	Collection Interval
	AVP but no valid Routing Entity Addresses were found.	
RxRbarResolFailUnsigned16Match	Number of Request messages received with an UNSIGNED16 value that did not match a provisioned address or address range.	5 min
RxRbarUnkApplId	Number of Request messages rejected due to an unknown Application ID.	5 min
TxRbarAbandonRequest	Number of Request messages that are abandoned	5 min

RxRbarDecodeFailureResol

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Request messages rejected due to a message decoding error.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and does not decode an AVP which extends beyond the length of the message indicated by the Message Length parameter in the message header.

Measurement Scope: Server Group

Recovery:

While parsing the message, the message content was inconsistent with the Message Length in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

RxRbarInvalidImsiMcc

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of times an AVP instance present in Diameter request message is rejected due to the MCC contained in the decoded IMSI falls within one of the configured Reserved MCC Ranges.

Collection Interval: 5 min

Peg Condition: Each time Diameter request message is rejected due to the MCC contained in the decoded IMSI falls within one of the configured Reserved MCC Ranges.

Measurement Scope: Server Group

Recovery:

1. Validate the ranges configured in the Reserved MCC Ranges table.
2. Verify that the MCC portion of the decodable IMSI received by RBAR do not fall within the configured Reserved MCC Ranges.
3. If the problem persists, contact the Tekelec *Customer Care Center*.

RxRbarResolFailAll

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received which did not resolve to a provisioned address or address range.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.

View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailCmdcode

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with an unknown Command Code.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and, after attempting to validate the ordered pair (Application ID and Command Code), the Command Code is unknown. RBAR invokes the routing exception handling procedure assigned to this Application ID and Routing Exception Type.

Measurement Scope: Server Group

Recovery:

The order pair (Application ID and Command Code) is not provisioned in the Address Resolutions routing configuration.

View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailDbFail

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of routing attempt failures due to internal database inconsistency failure.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and encounters a run-time database inconsistency.

Measurement Scope: Server Group

Recovery:

If this problem occurs, contact the *Customer Care Center*.

RxRbarResolFailImpiMatch

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with a valid IMPI that did not match a provisioned address or address range.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMPI and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailImpuMatch

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with a valid IMPU that did not match a provisioned address or address range.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMPU and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

.

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailImsiMatch

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with a valid IMSI that did not match a provisioned address or address range.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMSI and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailIpv4Match

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with an IPv4 Address that did not match a provisioned address or address range

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IPv4 Address and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailIpv6prefixMatch

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with an IPv6-Prefix Address that did not match a provisioned address or address range

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IPv6-Prefix Address and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailMsisdnMatch

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with a valid MSISDN that did not match a provisioned address or address range

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of MSISDN and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailNoAddrAvps

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received without a Routing Entity Address AVP.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message, with the number of AVPs searched–as defined by measurement RxRbarAvgAddrAvps for the message–as `0` and hence, a valid Routing Entity address cannot be found using any of the Routing Entity Types assigned to the ordered pair (Application ID and Command Code).

Measurement Scope: Server Group

Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailNoValidAddr

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with at least Routing Entity Address AVP but no valid Routing Entity Addresses were found.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message, with the number of AVPs searched–as defined by measurement RxRbarAvgAddrAvps for the message–as `> 0` but, a valid Routing Entity address cannot be found using any of the Routing Entity Types assigned to the ordered pair (Application ID and Command Code).

Measurement Scope: Server Group

Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarResolFailUnsigned16Match

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with an UNSIGNED16 value that did not match a provisioned address or address range.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of UNSIGNED16 and, using the provisioned individual addresses or address ranges, does not successfully resolve to a Destination.

Measurement Scope: Server Group

Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR** > **Configuration** > **Address Resolutions**.

RxRbarUnkApplId

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Request messages rejected due to an unknown Application ID.

Collection Interval: 5 min

Peg Condition: When a Request message received and the Application ID is not present in the RBAR configuration.

Measurement Scope: Server Group

Recovery:

The DSR Relay Agent forwarded a Request message to the address resolution application which contained an unrecognized Diameter Application ID in the header. Either a DSR Relay Agent application routing rule is misprovisioned or the Application ID is not provisioned in the RBAR routing configuration.

1. View the currently provisioned Diameter Application IDs by selecting **RBAR** > **Configuration** > **Applications**.
2. View the currently provisioned Application Routing Rules by selecting **Diameter** > **Configuration** > **Application Routing Rules**.

TxRbarAbandonRequest

Measurement Group: Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Request messages that are abandoned

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception "Abandon Request" is invoked

Measurement Scope: Server Group

Recovery:

No action required.

Address Resolution Performance measurements

The Address Resolution Performance measurement group is a set of measurements that provide performance information that is specific to a RBAR Application. These measurements allow you to determine how many messages are successfully forwarded and received to/from each RBAR Application.

Table 30: Address Resolution Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxRbarAvgMsgSize	Average size of Request message received.	5 min
RxRbarMsgs	Number of Diameter messages received by Range Based Address Resolution application.	5 min

Measurement Tag	Description	Collection Interval
RxRbarResolAll	Number of Addresses Successful Resolved to a Destination.	5 min
RxRbarResolAllMp	Number of Addresses Successful Resolved to a Destination by the MP.	5 min
RxRbarResolImpi	Number of Addresses Successful Resolved with Routing Entity type IMPI.	5 min
RxRbarResolImpu	Number of Addresses Successful Resolved with Routing Entity type IMPU.	5 min
RxRbarResolImsi	Number of Addresses Successful Resolved with Routing Entity type IMSI.	5 min
RxRbarResolIpv4	Number of Addresses Successful Resolved with Routing Entity type IPv4 Address.	5 min
RxRbarResolIpv6prefix	Number of Addresses Successful Resolved with Routing Entity type IPv6-Prefix Address.	5 min
RxRbarResolMsisdn	Number of Addresses Successful Resolved with Routing Entity type MSISDN.	5 min
RxRbarResolRateAvg	Average Addresses Successfully Resolved per second.	5 min
RxRbarResolRatePeak	Peak Addresses Successfully Resolved per second.	5 min
RxRbarResolSingleAddr	Number of Addresses Successful Resolved with an Individual Address.	5 min
RxRbarResolUnsigned16	Number of Addresses Successful Resolved with Routing Entity type UNSIGNED16.	5 min
TxRbarFwdDefaultDest	Number of Request message forwarding attempts using a Default Destination.	5 min
TxRbarFwdNochange	Number of Request message forwarding attempts without changing the message.	5 min

Measurement Tag	Description	Collection Interval
TxRbarFwdSuccess	Number of Request messages successfully forwarded (all reasons).	5 min
TxRbarMsgAttempt	Number of Request message forwarding attempts (all reasons).	5 min

RxRbarAvgMsgRate

Measurement Group: Address Resolution Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Average size of Request message received.

Collection Interval: 5 min

Peg Condition: Average calculated for each Request message received as defined by measurement *RxRbarMsgs*.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarMsgs

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received by RBAR.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and determines that the Application ID in the message header is defined in the routing configuration and valid.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolAll

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved to a Destination.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolAllMp

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Addresses Successful Resolved to a Destination by the MP.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and successfully resolves its Application ID, Command Code and Routing Entity to a Destination.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolImpi

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IMPI.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMPI and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolImpu

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IMPU.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMPU and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolImsi

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IMSI.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IMSI and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolIpv4

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IPv4 Address.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IPv4 Address and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolIpv6prefix

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IPv6-Prefix Address.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of IPv6-Prefix Address and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolMsisdn

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type MSISDN.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of MSISDN and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolRateAvg

No action required.

RxRbarResolRatePeak

Measurement Group: Address Resolution Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Peak Addresses Successfully Resolved per second

Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with average successfully resolved message rate, as defined by measurement *RxRbarResolRateAvg*, if the value exceeds the current value for this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolSingleAddr

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with an Individual Address.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message and uses the Address Exceptions to successfully resolve its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarResolUnsigned16

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type UNSIGNED16.

Collection Interval: 5 min

Peg Condition: When RBAR receives a Request message with a Routing Entity type of UNSIGNED16 and successfully resolves its Application ID, Command Code and Routing Entity to a Destination and forwards the message to the DSR Relay Agent.

Measurement Scope: Server Group

Recovery:

No action required.

TxRbarFwdDefaultDest

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message forwarding attempts using a Default Destination.

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception Forward route the message with a user-configurable Default Destination is invoked.

Measurement Scope: Server Group

Recovery:

No action required.

TxRbarFwdNoChange

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message forwarding attempts without changing the message.

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception `Forward route the message unchanged` is invoked.

Measurement Scope: Server Group

Recovery:

No action required.

TxRbarFwdSuccess

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages successfully forwarded (all reasons).

Collection Interval: 5 min

Peg Condition: Each time the application successfully enqueues a Request message on the DSR Relay Agent's Request Message Queue.

Measurement Scope: Server Group

Recovery:

If this value is less than measurement *TxRbarMsgAttempt*, then an internal resource error is occurring. Contact the *Customer Care Center*. if needed.

TxRbarMsgAttempt

Measurement Group: Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message forwarding attempts (all reasons).

Collection Interval: 5 min

Peg Condition: Each time the application attempts to enqueue a Request message on the DSR Relay Agent's Request Message Queue.

Measurement Scope: Server Group

Recovery:

No action required.

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.

Table 31: Application Routing Rule Measurements

Measurement Tag	Description	Collection Interval
RxApplRuleSelected	Number of times that an Application Routing Rule was selected to route a Request message	5 min
RxApplRuleFwdFailAll	Number of times that an Application Routing Rule was selected to route a Request message but the message was not successfully routed (all reasons)	5 min
RxApplRuleFwdFailUnavail	Number of times that an Application Routing Rule was selected to route a Request message but the message was not successfully routed because the DSR Application's	5 min

Measurement Tag	Description	Collection Interval
	Operational Status was Unavailable	
RxApplRuleDuplicatePriority	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.	5 min
RxArtSelected	Number of times that an application routing rule from ART-X was selected for routing a Request message	5 min

RxApplRuleSelected

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:

No action required.

RxApplRuleFwdFailAll

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:

No action required.

RxApplRuleFwdFailUnavail

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:

No action required.

RxApplRuleDuplicatePriority

Measurement Group: Peer 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:

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 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 Group: Server Group

Recovery:

No action required.

Charging Proxy Application (CPA) Exception measurements

The CPA Exception measurement group contains measurements that provide information about exceptions and unexpected messages and events that are specific to the CPA application. Measurements in this group include:

- Totals for unexpected/errors associated with message content
- Totals for unexpected/errors associated with message routing

Table 32: CPA Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvCpaMessageDecodeFail	The total number of diameter message decode failures.	5 min
EvCpaMissingAvp	The total number of diameter messages received without an AVP required for this application.	5 min
EvCpaOOS	The number of times the CPA was taken Out Of Service.	5 min
EvCpaSubResourceCongested	The total number of Sub-Resources that are determined to be in congestion.	5 min
EvCpaUnexpectedSess	The CPA has received an ACA-Start that already has a Session Binding Record.	5 min

Measurement Tag	Description	Collection Interval
EvCpaUnkDiameterAppId	The total number of diameter messages received with an unknown application ID.	5 min
RxCpaHaSubResourceUnavail	The number of times a Diameter message is received whose Session-Id hashes to a database partition that is unavailable.	5 min
RxCpaNon2xxAnswer	The number of Diameter Answer messages received with a non-2xx response code.	5 min
RxCpaOpStatusUnavail	The number of times a message is received and the CPA has an operational status of unavailable.	5 min
RxCpaUnexpected	The number of Unexpected Diameter message types received during the reporting interval.	5 min
TxCpaAnswerByCpa	The number of times an Answer is generated (not relayed) by the CPA.	5 min
TxCpaRteFailure	The number of messages sent by the CPA to the routing layer which failed to route successfully.	5 min

EvCpaMessageDecodeFail

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of diameter message decode failures.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever a Diameter message decode failure is detected.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaMissingAvp

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of diameter messages received without an AVP required for this application.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever a Diameter message is received without an AVP required for this application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaOOS

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times the CPA was taken Out Of Service.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA is taken Out Of Service either manually or automatically.

Measurement Scope: Network, NE, Server Group

Recovery:

1. This measurement indicates problems with the CPA. Logs and Alarms should be checked to determine the cause of the problem.
2. Contact the *Customer Care Center* for assistance.

EvCpaSubResourceCongested

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Congestion Level)

Description: The total number of Sub-Resources that are determined to be in congestion.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever SBR reports a congestion level either through a response or a polled query.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaUnexpectedSess

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The CPA has received an ACA-Start that already has a Session Binding Record.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an ACA-Start is received and a Session Binding Record already exists.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaUnkDiameterAppId

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of diameter messages received with an unknown application ID.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever a Diameter message is received with an unknown application ID.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaHaSubResourceUnavail

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Sub-Resource ID)

Description: The number of times a Diameter message is received whose Session-Id hashes to a database partition that is unavailable.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when a Diameter request hashes to a database partition that is unavailable.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaNon2xxxAnswer

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Diameter Answer messages received with a non-2xxx response code.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an unexpected Diameter answer with a non-2xxx response code is received.

Measurement Scope: Network, NE, Server Group

Recovery:

1. If this count is non-zero it could indicate a mis-configuration of Application Routing.
2. Contact the *Customer Care Center* for assistance.

RxCpaOpStatusUnavail

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times a message is received and the CPA has an operational status of unavailable.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when a Diameter Request is received when the operational status of the CPA is Unavailable.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaUnexpected

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Unexpected Diameter message types received during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an unexpected Diameter (ie; not an Accounting) message is received.

Measurement Scope: Network, NE, Server Group

Recovery:

1. If this count is non-zero it could indicate a mis-configuration of Application Routing.
2. Contact the *Customer Care Center* for assistance.

TxCpaAnswerByCpa

Measurement Group: CPA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times an Answer is generated (not relayed) by the CPA.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an error condition occurs that causes the CPA to generat an Answer and not relay one.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

TxCpaRteFailure

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of messages sent by the CPA to the routing layer which failed to route successfully.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA sends a message to the routing layer which fails to route successfully.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

Charging Proxy Application (CPA) Performance measurements

The CPA Performance measurement group contains measurements that provide performance information that is specific to the CPA application. Measurements in this group include:

- Totals for various expected/normal messages and events
- Totals for various expected/normal routing procedures invoked

Table 33: CPA Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxCpaAcaEvent	The number of Accounting Answer-Event messages received during the collection interval.	5 min
RxCpaAcaInterim	The number of Accounting Answer-Interim messages received during the collection interval.	5 min
RxCpaAcaStart	The number of Accounting Answer-Start messages received during the collection interval.	5 min
RxCpaAcaStop	The number of Accounting Answer-Stop messages received during the collection interval.	5 min
RxCpaAccounting	The number of Diameter Accounting messages received during the reporting interval.	5 min
RxCpaAcrEvent	The number of Accounting Request-Event messages received during the collection interval.	5 min
RxCpaAcrInterim	The number of Accounting Request-Interim messages received during the collection interval.	5 min
RxCpaAcrStart	The number of Accounting Request-Start messages received during the collection interval.	5 min
RxCpaAcrStop	The number of Accounting Request-Stop messages received during the collection interval.	5 min
RxCpaMsgProcessed	The total number of Diameter messages (Request or Answer)	5 min

Measurement Tag	Description	Collection Interval
	received during the reporting interval.	
TxCpaAnswerMsgToDrl	The number of Answers sent to DRL layer by CPA during the collection interval.	5 min
TxCpaMsgCopyInd	The number of messages sent by the CPA to the routing layer with message copy indication set.	5 min
TxCpaRequestMsgToDrl	The number of Requests sent to DRL layer by CPA during the collection interval.	5 min
TxCpaTraceInd	The number of messages sent by the CPA to the routing layer with trace indication set.	5 min

RxCpaAcaEvent

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Answer-Event messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Answer-Event message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcaInterim

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Answer-Interim messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Answer-Interim message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcaStart

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Answer-Start messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Answer-Start message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcaStop

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Answer-Stop messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Answer-Stop message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAccounting

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Diameter Accounting messages received during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when a Diameter Accounting message is received.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcrEvent

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Request-Event messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Request-Event message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcrInterim

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Request-Interim messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Request-Interim message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcrStart

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Request-Start messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Request-Start message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaAcrStop

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Accounting Request-Stop messages received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when an Accounting Request-Stop message is received by the CPA application.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaMsgProcessed

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of Diameter messages (Request or Answer) received during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever a Diameter message (Request or Answer) is received.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

TxCpaAnswerMsgToDrl

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Answers sent to DRL layer by CPA during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever CPA sends an Answer to DRL during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

TxCpaMsgCopyInd

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of messages sent by the CPA to the routing layer with message copy indication set.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA sends a message to the routing layer with the message copy indication set.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

TxCpaRequestMsgToDrl

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Requests sent to DRL layer by CPA during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever CPA sends a Request to DRL during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

TxCpaTraceInd

Measurement Group: CPA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of messages sent by the CPA to the routing layer with trace indication set.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA sends a message to the routing layer with the trace indication set.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

Charging Proxy Application (CPA) Session DB measurements

The CPA Session DB measurement group contains measurements that provide information about events that occur when the CPA queries the Session Binding Repository:

- Performance related measurements for SBR queries
- Exceptions and unexpected events related to SBR query processing

Table 34: CPA Session DB Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvCpaNoSbrAccess	The number of queries by the CPA to the SBR where the SBR is inaccessible.	5 min
EvCpaSbrAvgRespTime	The average response time for a stateful SBR transaction.	5 min
EvCpaSbrCreateSess	The number of sessions created by the CPA on the SBR during the collection interval.	5 min

Measurement Tag	Description	Collection Interval
EvCpaSbrDeleteSess	The number of sessions deleted by the CPA on the SBR during the collection interval.	5 min
EvCpaSbrPeakRespTime	The peak response time for SBR queries during the reporting interval.	5 min
EvCpaSbrQryError	The number of queries initiated by the CPA to the SBR that resulted in an error condition during the collection interval.	5 min
EvCpaSbrQryMatch	The number of queries initiated by the CPA to the SBR that resulted in a matching condition during the collection interval.	5 min
EvCpaSbrQryNoMatch	The number of queries initiated by the CPA to the SBR that resulted in a no match condition during the collection interval.	5 min
EvCpaSbrRespTime	This measurement groups responses to SBR queries by the amount of round trip time they took to process. Each bucket will represent the number of responses processed within that time interval.	5 min
EvCpaSbrUpdateSess	The number of update session requests sent by the CPA to the SBR during the collection interval. The value does not include created sessions.	5 min
RxCpaUndeliveredMsg	The total number of messages that ComAgent could not send or for which it did not receive a response.	5 min
TxCpaSbrQueryTot	The total number of queries (reads / creates / updates / deletes) sent from the CPA to the SBR during the reporting interval.	5 min

EvCpaNoSbrAccess

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of queries by the CPA to the SBR where the SBR is inaccessible.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA attempts a query when the SBR is inaccessible.

Measurement Scope: Network, NE, Server Group

Recovery:

1. The SBR could be Out Of Service or temporarily down.
2. Contact the *Customer Care Center* for assistance.

EvCpaSbrAvgRespTime

Measurement Group: CPA Session DB

Measurement Type: Average

Measurement Dimension: Single

Description: The average response time for a stateful SBR transaction.

Collection Interval: 5 min

Peg Condition: This measurement is the average response time for SBR transactions.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrCreateSess

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of sessions created by the CPA on the SBR during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA creates a new session based on the session identifier.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrDeleteSess

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of sessions deleted by the CPA on the SBR during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever CPA deletes a session on the SBR during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrPeakRespTime

Measurement Group: CPA Session DB

Measurement Type: Max

Measurement Dimension: Single

Description: The peak response time for SBR queries during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement tracks the maximum response time for an SBR query in milliseconds for the reporting interval.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrQryErr

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of queries initiated by the CPA to the SBR that resulted in an error condition during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA initiates a query to the SBR and receives an error response.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrQryMatch

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of queries initiated by the CPA to the SBR that resulted in a matching condition during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA initiates a query to the SBR and finds a match based on the session identifier.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrQryNoMatch

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of queries initiated by the CPA to the SBR that resulted in a no match condition during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the initiates a query (read, create, update, delete) to the and finds no match based on the session identifier.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrResponseTime

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Arrayed (by Response Time Interval)

Description: This measurement groups responses to SBR queries by the amount of round trip time they took to process. Each bucket will represent the number of responses processed within that time interval.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged for every SBR response received.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

EvCpaSbrUpdateSess

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of update session requests sent by the CPA to the SBR during the collection interval. The value does not include created sessions.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when the CPA sends an update request to the SBR.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaUndeliveredMsg

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of messages that ComAgent could not send or for which it did not receive a response.

Collection Interval: 5 min

Peg Condition: This measurement will be pegged whenever a ComAgent invokes the Undelivered Message callback.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

TxCpaSbrQueryTot

Measurement Group: CPA Session DB

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of queries (reads / creates / updates / deletes) sent from the CPA to the SBR during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement is the total number of queries sent by the CPA to the SBR.

Measurement Scope: Network, NE, Server Group

Recovery:

No action 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.

Table 35: Communication Agent Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
CADataFIFOQueueFul	StackEvents discarded due to ComAgent DataFIFO queue full condition.	30 min
CADSTxDscrdCong	Number of egress stack events discarded because the congestion level of the connection exceeded the stack events' priority level.	30 min
CAHSRsrcErr	Number of times that ComAgent receives in a heartbeat stack event status concerning a known Resource but an unknown Sub-Resource.	30 min
CAHSTxDscrdCongSR	Number of stack events discarded due to HA Service Sub-Resource congestion.	30 min
CAHSTxDscrdIntErrSR	Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.	30 min
CAHSTxDscrdUnavailSR	Number of stack events discarded because they were submitted to an Unavailable	30 min

Measurement Tag	Description	Collection Interval
	Sub-Resource of a given Resource.	
CAHSTxDscrdUnknownSR	Number of egress stack events discarded because they referred to a known Resource and an unknown Sub-Resource.	30 min
CAHSTxDscrdUnkwnRsrc	Number of egress stack events discarded because they referred to an unknown Resource.	30 min
CAHSTxRsrc	Number of egress stack events that were routed to a known Resource.	30 min
CAMxFIFOQueueFul	StackEvents discarded due to ComAgent MxFIFO queue full condition.	30 min
CARsrcPoolFul	ComAgent internal resource pool exhaustion condition	
CARSTxDscrdCong	Number of stack events discarded due to Routed Service congestion.	30 min
CARSTxDscrdSvcUnavail	Number of stack events discarded because they were submitted to an Unavailable Routed Service.	30 min
CARxDiscUnexpEvent	Number of ingress events discarded because it was unexpected in the connection operational state.	30 min
CARxDscrdConnUnavail	Number of User Data ingress events discarded because connection was not in-service.	30 min
CARxDscrdDecodeFailed	Number of ingress events discarded because failed to deserialize (event not part of stack service language).	30 min
CARxDscrdIncompat	Number of ingress events discarded because an Incompatible header version is received.	30 min
CARxDscrdInternalErr	Number of ingress events discarded because of other unexpected internal processing error.	30 min

Measurement Tag	Description	Collection Interval
CARxDscrdLayerSendFail	Number of User Data ingress events discarded because layer's sendTo failed.	30 min
CARxDscrdMsgLenErr	Number of ingress events discarded as it doesn't contain enough bytes (less than event header bytes).	
CARxDscrdUnkServer	Number of ingress events discarded because the origination server was unknown/not configured.	30 min
CARxDscrdUnkStkLyr	Number of User Data ingress events discarded because stack layer is not known.	30 min
CARxMsgUnknown	Number of ingress events discarded because stack event was unknown.	30 min
CAStackQueueFul	StackEvents discarded due to ComAgent task queue full condition.	30 min
CATransDscrdInvCorrId	Number of received stack events that were received and discarded because they did not correlate with a pending transaction.	30 min
CATransDscrdStaleErrRsp	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.	30 min
CATransEndAbnorm	Number of reliable transactions that terminated abnormally.	30 min
CATransEndAbnormRateAvg	Average rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndAbnormRateMax	Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndAnsErr	Number of reliable transactions initiated by local User Layers that ended with an error	30 min

Measurement Tag	Description	Collection Interval
	response from a destination server.	
CATransEndErr	Number of reliable transactions initiated by local User Layers that ended abnormally with an error response from a destination server.	30 min
CATransEndNoResources	Number of reliable transactions initiated by local User Layers that ended abnormally due to lack of resources.	30 min
CATransEndNoResponse	Number of reliable transactions initiated by local User Layers that ended abnormally due to a timeout waiting for a response.	30 min
CATransEndUnkwnSvc	Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to an unknown service.	30 min
CATransEndUnregSvc	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.	30 min
CATransNoReTxMaxTTL	Number of reliable transactions abnormally ended because of Max Time to live exceeded without any retransmits.	30 min
CATransRetx	Number of times stack events were retransmitted.	30 min
CATransReTxExceeded	Number of reliable transactions abnormally ended because of Max number of Retries exceeded.	30 min
CATransStaleSuccessRsp	Number of times that a success response was received from an unexpected server and was accepted to end a transaction.	30 min
CATransTTLExceeded	Number of reliable transactions abnormally ended because of Max Time to live exceeded.	30 min

Measurement Tag	Description	Collection Interval
CATxDscrdConnUnAvail	Number of User Data egress events discarded because connection was not in-service(down/blocked/not aligned).	30 min
CATxDscrdDestUserIncmpat	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)	30 min
CATxDscrdEncodeFail	Number of User Data egress events discarded because of serialization failures	30 min
CATxDscrdInternalErr	Number of egress events discarded because of other unexpected internal processing error.	30 min
CATxDscrdMxSendFail	Number of User Data egress events discarded because of failure reported by MxEndpoint	30 min
CATxDscrdUnknownSvc	Number of non-reliable and non-request (G=0 or R=0) egress stack events discarded because they refer to an unknown service.	30 min
CATxDscrdUnkServer	Number of egress events discarded because the destination server was unknown/not configured.	30 min
CATxDscrdUnregSvc	Number of egress stack events discarded because they reference a known service that has no registered User Layer.	30 min

CADataFIFOQueueFul

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. Contact the *Customer Care Center* for assistance.

CADSTxDscrdCong

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:

When this measurement is increasing, it is an indication that the product is experiencing overload.

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.

2. Contact the *Customer Care Center* for assistance.

CAHSRsrcErr

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. Contact the Tekelec *Customer Care Center* for assistance.

CAHSTxDscrdCongSR

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 product'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. Contact the *Customer Care Center* for assistance.

CAHSTxDscrdIntErrSR

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, contact the *Customer Care Center*.

CAHSTxDscrdUnavailSR

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** > **Comamunication 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. Contact the *Customer Care Center* for assistance.

CAHSTxDscrdUnknownSR

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** > **Comamunication Agent** > **Maintenance** > **HA Services Status** to verify that all HA Service Sub-Resources expected by local applications are present and operating.
2. Contact the *Customer Care Center* for assistance.

CAHSTxDscrdUnkwnRsrc

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. Use **Main Menu** > **Comamunication Agent** > **Maintenance** > **HA Services Status** to verify that all HA Service Sub-Resources expected by local applications are present and operating.
2. Contact the *Customer Care Center* for assistance.

CAHSTxRsrc

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:

No action required.

CAMxFIFOQueueFul

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. Contact the *Customer Care Center* for assistance.

CARsrcPoolFul

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:

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 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. Contact the *Customer Care Center* for assistance.

CARSTxDscrdSvcUnavail

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* for assistance.

CARxDiscUnexpEvent

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:

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.

CARxDscrdConnUnavail

Measurement Group: ComAgent Exception

Measurement Type: Simple

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:

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 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:

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 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:

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 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:

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 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:

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 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:

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 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:

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 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:

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 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:

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 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. Contact the *Customer Care Center* for assistance.

CATransDscrdInvCorrId

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:

This measurement indicates that one or more destination servers are either responding to requests after a transaction has ended or are sending invalid responses. Contact the *Customer Care Center* for assistance.

CATransDscrdStaleErrRsp

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.

Measurement Scope: Server

Recovery:

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

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. Contact the *Customer Care Center* for assistance.

CATransEndAbnorm

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. Contact the *Customer Care Center* for assistance.

CATransEndAbnormRateAvg

Measurement Group: ComAgent Performance

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 an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.

Measurement Scope: Server

Recovery:

This measurement provides the average rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransEndAbnormRateMax

Measurement Group: ComAgent Performance

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 an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.

Measurement Scope: Server

Recovery:

This measurement provides the maximum rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransEndAnsErr

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:

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 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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* for assistance.

CATransEndNoResources

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* for assistance.

CATransEndNoResponse

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* for assistance.

CATransEndUnkwnSvc

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.

Measurement Scope: Server

Recovery:

This measurement indicates improper configuration of ComAgent and/or a User Layer application.

1. Use **Main Menu** > **Communication Agent** > **Configuration** > **Routed Services** to confirm that all services expected by local applications are present.
2. Contact the *Customer Care Center* for assistance.

CATransEndUnregSvc

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:

A non-zero value in this measurement indicates a software malfunction.

Contact the *Customer Care Center* for assistance.

CATransNoReTxMaxTTL

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* if assistance is needed

CATransRetx

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* for assistance.

CATransReTxExceeded

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* if assistance is needed

CATransStaleSuccessRsp

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.

Measurement Scope: Server

Recovery:

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.

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to diagnose stale responses.
2. Contact the *Customer Care Center* for assistance.

CATransTTLExceeded

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.

Measurement Scope: Server

Recovery:

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.

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. Contact the *Customer Care Center* if assistance is needed

CATxDscrdConnUnAvail

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:

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 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:

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 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:

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 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:

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 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:

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 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. Contact the *Customer Care Center* for assistance.

CATxDscrdUnkServer

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:

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 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:

A non-zero measurement indicates that a local application is malfunctioning and is attempting to use a service for which it has not registered. Contact the *Customer Care Center* 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.

Table 36: Communication Agent Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
CAAvgDataFIFOQueueUtil	Average percentage of ComAgent DataFIFO Queue Utilization	30 min
CAAvgMxFIFOQueueUtil	Average percentage of ComAgent MxFIFO Queue Utilization	30 min
CAAvgQueueUtil	Average percentage of Queue Utilization.	30 min

Measurement Tag	Description	Collection Interval
CAAvgRsrcPoolUtil	Average percentage of internal resource pool utilization	30 min
CAAvgRxStackEvents	Average Number of User Data ingress events received.	30 min
CAAvgTxStackEvents	Average Number of User Data egress events received from stacks to deliver it to remote.	30 min
CADSTx	Number of User Data egress events specifically for the default Direct Service.	30 min
CAHSTxRsrc	Number of egress stack events that were routed to a known Resource.	30 min
CAHSTxRsrcRateAvg	Average rate per second of egress stack events routed to a known Resource.	30 min
CAHSTxRsrcRateMax	Maximum rate per second of egress stack events routed to a known Resource	30 min
CAPeakDataFIF0QueueUtil	Maximum percentage of ComAgent DataFIFO Queue Utilization	30 min
CAPeakMxFIFOQueueUtil	Maximum percentage of ComAgent MxFIFO Queue Utilization	30 min
CAPeakQueueUtil	Maximum percentage of Queue Utilization.	30 min
CAPeakRsrcPoolUtil	Maximum percentage of internal resource pool utilization	30min
CAPeakRxStackEvents	Maximum Number of User Data ingress events received.	30 min
CAPeakTxStackEvents	Maximum Number of User Data egress events received from stacks to deliver it to remote.	30 min
CARSTx	Number of stack events submitted to a Routed Service for routing.	30 min
CARx	Number of User Data ingress events received from a peer server.	30 min

Measurement Tag	Description	Collection Interval
CARxSuccess	Number of User Data ingress events successfully routed to local layers.	30 min
CATransEndAbnorm	Number of reliable transactions that terminated abnormally.	30 min
CATransEndAbnormRateAvg	Average rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndAbnormRateMax	Maximum rate per second that ComAgent transactions ended abnormally during the collection interval.	30 min
CATransEndNorm	Number of reliable transactions initiated by local User Layers that ended normally with a response from a destination server.	30 min
CATransPendingAvg	Average number of allocated pending transaction records over the collection interval.	30 min
CATransPendingMax	Maximum number of allocated pending transaction records.	30 min
CATransRateAvg	Average rate per second that ComAgent transactions were started during the collection interval.	30 min
CATransRateMax	Maximum rate per second that ComAgent transactions were started during the collection interval.	30 min
CATransStarted	Number of reliable transactions initiated by local User Layers.	30 min
CATransTimeAvg	Average transaction life-time in milliseconds.	30 min
CATransTimeMax	Maximum transaction life-time in milliseconds.	30 min
CATx	Number of User Data egress events received on Communication Agent task queue from local stacks to deliver it to a peer server.	30 min

Measurement Tag	Description	Collection Interval
CATxSuccess	Number of User Data egress events successfully delivered to a peer server.	30 min

CAAvgDataFIFOQueueUtil

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. Contact the *Customer Care Center* for assistance.

CAAvgMxFIFOQueueUtil

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. Contact the *Customer Care Center* for assistance.

CAAvgQueueUtil

Measurement Group: ComAgent Exception

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. Contact the *Customer Care Center* for assistance.

CAAvgRsrcPoolUtil

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:

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 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:

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 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:

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 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:

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 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:

No action required.

CAHSTxRsrcRateAvg

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:

No action required.

CAHSTxRsrcRateMax

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:

No action required.

CAPeakDataFIFOQueueUtil

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. Contact the *Customer Care Center* for assistance.

CAPeakMxFIFOQueueUtil

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. Contact the *Customer Care Center* for assistance.

CAPeakQueueUtil

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. Contact the *Customer Care Center* for assistance.

CAPeakRsrcPoolUtil

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:

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 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:

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 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:

No action required.

This value provides a measure of Peak Value during the interval, for number of User Data messages transmitted to remote.

CARSTx

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:

No action necessary

CARx

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:

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

CARxSuccess

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:

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 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. Contact the *Customer Care Center* for assistance.

CATransEndAbnormRateAvg

Measurement Group: ComAgent Performance

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 an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.

Measurement Scope: Server

Recovery:

This measurement provides the average rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransEndAbnormRateMax

Measurement Group: ComAgent Performance

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 an exponential smoothing algorithm. The average transaction failure rate is a running average, smoothed over approximately 10 seconds.

Measurement Scope: Server

Recovery:

This measurement provides the maximum rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransEndNorm

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:

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 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:

No action necessary.

CATransPendingMax

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:

No action necessary.

CATransRateAvg

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 an exponential smoothing algorithm. The average transaction rate is a running average, smoothed over approximately 10 seconds.

Measurement Scope: Server

Recovery:

This measurement provides the average rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransRateMax

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 an exponential smoothing algorithm. The average transaction rate is a running average, smoothed over approximately 10 seconds.

Measurement Scope: Server

Recovery:

This measurement provides the maximum rate per second that ComAgent transactions were started. This measurement is useful during trouble shooting when compared to other measurements.

No action necessary.

CATransStarted

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:

No action necessary.

CATransTimeAvg

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:

No action necessary.

CATransTimeMax

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:

No action necessary.

CATx

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:

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.

CATxSuccess

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:

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.

Computer Aided Policy Making (CAPM) measurements

The Computer-Aided Policy Making (CAPM) measurement report contains usage-based measurements related to the Diameter Mediation feature.

Table 37: CAPM Measurement Report Fields

Measurement Tag	Description	Collection Interval
CAPM_Temp_Invoked	Number of times a Rule Template has been invoked. This counter is incremented on a per Rule Template basis every time the Rule Template is processed.	5 min
CAPM_CondSet_True	Number of times a condition set has been evaluated to True. This counter is incremented on a per Rule Template basis every time all the conditions of the condition set match.	5 min

Measurement Tag	Description	Collection Interval
CAPM_Action_Set_Fails	Number of times a failure has occurred while executing the action set. This counter is incremented on a per Rule Template basis every time some of the actions fails. **Note:** This counter is incremented only once even if several actions within an action set have failed.	5 min
CAPM_MsgCopyTriggered	Number of times the MsgCopy action has been invoked successfully	5 min

CAPM_Temp_Invoked

Measurement Group: CAPM

Measurement Type: Simple

Measurement Dimension: Arrayed (by Mediation Rule Template ID)

Description: Indicates the number of times a Rule Template has been invoked. This counter is incremented on a per Rule Template basis every time the Rule Template is processed.

Collection Interval: 5 min

Peg Condition: A Rule Template is invoked during the message processing.

Measurement Scope: Server Group

Recovery:

1. Verify that the Rule Template was set to Test or Active state and was assigned to the correct Execution Trigger.
2. Verify the conditions of the Rule Template were properly set and the provisioned routing or/and mediation data matches the incoming message.
3. Verify that alarm *25000 - Rule Template failed to be updated* is not raised.

CAPM_CondSet_True

Measurement Group: CAPM

Measurement Type: Simple

Measurement Dimension: Arrayed (by Mediation Rule Template ID)

Description: Indicates the number of times a condition set has been evaluated to True. This counter is incremented on a per Rule Template basis every time all the conditions of the condition set match.

Collection Interval: 5 min

Peg Condition: A Condition Set matches during the message processing.

Measurement Scope: Server Group

Recovery:

1. Verify that the Rule Template was set to Test or Active state and was assigned to the correct Execution Trigger.
2. Verify the conditions of the Rule Template were properly set and the provisioned routing or/and mediation data matches the incoming message.
3. Also verify that the alarm *25000 - Rule Template failed to be updated* is not raised.

CAPM_Action_Set_Fails

Measurement Group: CAPM

Measurement Type: Simple

Measurement Dimension: Arrayed (by Mediation Rule Template ID)

Description: Indicates the number of times a failure has occurred while executing the action set. This counter is incremented on a per Rule Template basis every time some of the actions fails.

Note: This counter is incremented only once even if several actions within an action set have failed.

Collection Interval: 5 min

Peg Condition: At least one action within an Action Set has failed.

Measurement Scope: Server Group

Recovery:

Verify that the actions are set correctly, there are enough system resources to perform the actions, and the actions refer to the part of the incoming message that is available.

CAPM_MsgCopyTriggered

Measurement Group: CAPM

Measurement Type: Simple

Measurement Dimension: Arrayed (by Mediation Rule Template ID)

Description: The number of times the MessageCopy action has been invoked successfully.

Collection Interval: 5 min

Peg Condition: Each time the MessageCopy action has been invoked successfully.

Measurement Scope: Server Group

Recovery:

No action required

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

Table 38: Connection Congestion Measurement Report Fields

Measurement Tag	Description	Collection Interval
ConnOnsetCL1	The number of times the connection experienced the onset of CL1.	5 min
ConnOnsetCL2	The number of times the connection experienced the onset of CL2.	5 min
ConnOnsetCL3	The number of times the connection experienced the onset of CL3.	5 min
ConnOnsetCL4	The number of times the connection experienced the onset of CL4.	5 min
EvEmrCongestionOnset	Number of times an EMR Congestino Level was advanced	5 min
EvRemoteBusyCongested	Number of times Remote Busy Congestion occurred.	5 min
EvSmoothedEmrPeak	Smoothed EMR Peak.	5 min
EvSmoothedEmrAvg	Smoothed EMR Average.	5 min
RxRejectedConnCongestion	Number of Request messages from a downstream peer rejected by a Local Node because of Diameter Connection Congestion.	5 min
TmConnInCL1	Total amount of time (in seconds) the connection experienced CL1.	5 min
TmConnInCL2	Total amount of time (in seconds) the connection experienced CL2.	5 min
TmConnInCL3	Total amount of time (in seconds) the connection experienced CL3.	5 min
TmConnInCL4	Total amount of time (in seconds) the connection experienced CL4.	5 min

ConnOnsetCL1

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection experienced the onset of CL1.

Collection Interval: 5 min

Peg Condition: Each time the congestion level for a connection changes from CL0 to CL1

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. Check to see if the Remote Busy Abatement Timeout is too small.
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

ConnOnsetCL2

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection experienced the onset of CL2.

Collection Interval: 5 min

Peg Condition: Each time the congestion level for a connection changes from CL0 or CL1 to CL2.

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. Check to see if the Remote Busy Abatement Timeout is too small.
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

ConnOnsetCL3

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection experienced the onset of CL3.

Collection Interval: 5 min

Peg Condition: Each time the congestion level for a connection changes from CL0, CL1, or CL2 to CL3

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. Check to see if the Remote Busy Abatement Timeout is too small.
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

ConnOnsetCL4

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection experienced the onset of CL4.

Collection Interval: 5 min

Peg Condition: Each time the congestion level for a connection changes from CL0, CL1, CL2, or CL3 to CL4.

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, determine if either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. Check to see if the Remote Busy Abatement Timeout is too small.
3. Verify whether or not other connections to the adjacent Diameter node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. Examine if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.

EvEmrCongestionOnset

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Number of times an EMR Congestion Level was advanced

Collection Interval: 5 min

Peg Condition Each time the EMR Congestion Level is advanced

Measurement Scope:

Recovery: Site

1. Verify the "Maximum EMR" for the connection is set sufficiently high.
2. Verify the EMR onset/abatement thresholds are properly adjusted. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "Smoothing Factor" parameter for the connection is properly adjusted. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the connection is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Check to see if other connections to the adjacent Diameter Node are out of service. Adjacent Diameter nodes being out of service can cause more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
6. Check to see if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
7. If the problem persists, contact the *Customer Care Center*.

EvRemoteBusyCongestion

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Number of times Remote Busy Congestion occurred.

Collection Interval: 5 min

Peg Condition: Each time the Remote Busy Congestion Level changed from CL0 to either CL1, CL2 or CL3.

Measurement Scope: Site

Recovery:

1. Verify the "Maximum EMR" for the connection is set sufficiently high.
2. Verify the EMR onset/abatement thresholds are properly adjusted. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.

3. Verify the "Smoothing Factor" parameter for the connection is properly adjusted. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "Remote Busy Abatement Timeout" for the connection is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Check to see if other connections to the adjacent Diameter Node are out of service. Adjacent Diameter nodes being out of service can cause more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
6. Check to see if the connection is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
7. If the problem persists, contact the *Customer Care Center*.

EvSmoothedEmrAvg

Measurement Group: Connection Congestion

Measurement Type: Average

Measurement Dimension: Arrayed (by Connection ID)

Description: Average of the “Smoothed EMR” calculations made during the collection interval.

Collection Interval: 5 min

Peg Condition: A “Smoothed EMR” calculation St is periodically calculated (every 90ms). Each time St is calculated, then the “Average Smoothed EMR” measurement shall be updated. For example, if 3 Smoothed EMR values were calculated during the collection interval – 10, 14 and 9 respectively, then the “Average Smoothed EMR” would be: 11 ((10+14+ 9)/3)

Measurement Scope: Site

Recovery:

No action necessary.

EvSmoothedEmrPeak

Measurement Group: Connection Congestion

Measurement Type: Max

Measurement Dimension: Arrayed (by Connection ID)

Description: Peak “Smoothed EMR” calculation made during the collection interval.

Collection Interval: 5 min

Peg Condition: A “Smoothed EMR” calculation St is periodically calculated (every 90ms). If the new St exceeds any previous St-k value for the collection interval, then this measurement will be updated with the new St value. For example, if 3 Smoothed EMR values were calculated during the collection interval – 10, 14 and 9 respectively, then the “Peak Smoothed EMR” would be: 14=Max(10, 14, 9)

Measurement Scope: Site

Recovery:

No action necessary.

RxRejectedConnCongestion

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:

No action required.

TmConnInCL1

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time (in seconds) the connection experienced CL1.

Collection Interval: 5 min

Peg Condition: A "time duration interval" is determined as follows:

The "time duration interval" starts when one of the following occurs:

- New "collection interval" for the measurement begins and the connection congestion level is CL1.
- Connection congestion level changes to CL1.

The "time duration interval" stops when one of the following occurs:

- The collection interval for the measurement ends.
- The connection congestion level changes from CL1 to another congestion level.

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.

4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact the *Customer Care Center* for further assistance.

TmConnInCL2

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time (in seconds) the connection experienced CL2.

Collection Interval: 5 min

Peg Condition: A "time duration interval" is determined as follows:

The "time duration interval" starts when one of the following occurs:

- New "collection interval" for the measurement begins and the connection congestion level is CL2.
- Connection congestion level changes to CL2.

The "time duration interval" stops when one of the following occurs:

- The collection interval for the measurement ends.
- The connection congestion level changes from CL2 to another congestion level.

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact the *Customer Care Center* for further assistance.

TmConnInCL3

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time (in seconds) the connection experienced CL3.

Collection Interval: 5 min

Peg Condition: A "time duration interval" is determined as follows:

The "time duration interval" starts when one of the following occurs:

- New "collection interval" for the measurement begins and the connection congestion level is CL3.
- Connection congestion level changes to CL3.

The "time duration interval" stops when one of the following occurs:

- The collection interval for the measurement ends.
- The connection congestion level changes from CL3 to another congestion level.

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.
4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact the *Customer Care Center* for further assistance.

TmConnInCL4

Measurement Group: Connection Congestion

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time (in seconds) the connection experienced CL4.

Collection Interval: 5 min

Peg Condition: A "time duration interval" is determined as follows:

The "time duration interval" starts when one of the following occurs:

- New "collection interval" for the measurement begins and the connection congestion level is CL4.
- Connection congestion level changes to CL4.

The "time duration interval" stops when one of the following occurs:

- The collection interval for the measurement ends.
- The connection congestion level changes from CL4 to another congestion level.

Measurement Scope: Server Group

Recovery:

1. If EMR Throttling is enabled for the connection, either the maximum EMR may be set too high or the onset/abatement thresholds need adjustment.
2. The "Remote Bust Abatement Timeout" may be too small.
3. This problem can be caused if other connections to the adjacent Diameter Node are out of service, thus causing more traffic to be sent on this connection than what the adjacent Diameter Node can support on a per-connection basis.

4. The connection may be over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to this connection.
5. Contact the *Customer Care Center* for further assistance.

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.

Table 39: Connection Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvConnCerValFail	The number of times a CER contained invalid or unsupported AVP or AVP value.	5 min
EvConnCexIpChkFail	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).	5 min
EvConnCnxFail	Number of times the transport connection attempt failed. This includes only unsuccessful attempts to connect to the peer; it does not include failure of established connections.	5 min
EvConnDnsFail	Number of times an attempt to resolve a peer's FQDN to an IP address via DNS failed.	5 min
EvConnFarEndClose	Number of times the far end closed the connection.	5 min
EvConnManClose	Number of times the connection was manually closed via administratively Disabling the connection locally.	5 min
EvConnPeerNumIpFail	The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.	5 min

Measurement Tag	Description	Collection Interval
EvConnRelease	The number of times the connection was terminated based on a connection release request from DRL	5 min
EvConnSockInitFail	Number of times the socket initialization failed.	5 min
EvConnTransFail	The number of times the connection was closed due to SCTP/TCP transport failure.	5 min
RxConnGapAckBlocks	The number of gap acknowledgement blocks received on the SCTP connection.	5 min
TxConnRetransDataChunks	The number of retransmitted data chunks sent on the SCTP connection.	5 min
RxConnDupPkts	The number of duplicate packets received on the TCP connection.	5 min
TxConnRetransSegs	The number of retransmitted segments sent on the TCP connection.	5 min
TxConnSendFail	Number of times the transport send failed for any message on an established connection. When this occurs, the transport connection will NOT be disconnected.	5 min

EvConnCerValFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: CER contained invalid or unsupported AVP or AVP value.

Collection Interval: 5 min

Peg Condition: Inband-Security AVP value in CER was other than 0 (NO_INBAND_SECURITY).

Measurement Scope: Server Group

Recovery:

1. Disable peer's use of inband security.
2. If the problem persists, contact the *Customer Care Center*.

EvConnCexIpChkFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

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).

Collection Interval: 5 min

Peg Condition: On receipt of CER/CEA message from the peer for which 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).

Measurement Scope: Server Group

Recovery:

1. Diagnose peer to resolve inconsistency.
2. If the problem persists, contact the *Customer Care Center*.

EvConnCnxFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the transport connection attempt failed. This includes only unsuccessful attempts to connect to the peer; it does not include failure of established connections.

Collection Interval: 5 min

Peg Condition: Pegged when the DSR attempts to initiate a connection to a peer and fails.

Measurement Scope: Server Group

Recovery:

1. If this measurement indicates an excessive number of failed connection attempts, check that the peer is operational, and that it is accepting connections on the SCTP/TCP listen port configured for the Peer Node.
2. Contact the *Customer Care Center* for assistance if needed.

EvConnDnsFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times an attempt to resolve a peer's FQDN to an IP address via DNS failed.

Collection Interval: 5 min

Peg Condition: Pegged when a connection is closed without the peer sending a DPR.

Measurement Scope: Server Group

Recovery:

1. If this measurement indicates an excessive number of DNS resolution failures, examine the DNS configuration values to determine if the correct DNS servers are being queried.
2. Examine the DNS configuration of the configured DNS servers.
3. Contact the *Customer Care Center* for assistance if needed.

EvConnFarEndClose

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the far end closed the connection.

Collection Interval: 5 min

Peg Condition: Pegged when the peer closes the connection.

Measurement Scope: Server Group

Recovery:

If this measurement indicates an excessive number of peer disconnects, the Alarm History and measurements *RxConnDpr*, *RxConnDwr*, and *TxConnDwa* should be examined to determine the reason for the peer disconnects.

EvConnManClose

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection was manually closed via administratively disabling the connection locally.

Collection Interval: 5 min

Peg Condition: Pegged when a user disables a connection from the GUI.

Measurement Scope: Server Group

Recovery:

No action required.

EvConnPeerNumIpFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The peer has advertised in the INIT/INIT_ACK chunk a number of IP addresses different from the number of IP addresses the peer has been configured with in the respective connection object.

Collection Interval: 5 min

Peg Condition: The peer advertised a different number of IP addresses than configured.

Measurement Scope: Server Group

Recovery:

Check the peer configuration on the local node and the networking configuration on the peer itself with regard to which IP addresses the peer shall advertise using the **Diameter > Configuration > System Options** page.

EvConnRelease

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the connection was terminated based on a connection release request from DRL.

Collection Interval: 5 min

Peg Condition: Pegged when a connection terminated successfully on request from DRL.

Measurement Scope: Server Group

Recovery:

No action necessary.

EvConnSockInitFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the socket initialization failed.

Collection Interval: 5 min

Peg Condition: Pegged when the DSR attempts to apply the SCTP/TCP socket options to a peer connection and fails.

Measurement Scope: Server Group

Recovery:

Check the SCTP/TCP options in the Connection Configuration Set for the connection and correct them.

EvConnTransFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the transport connection was closed due to SCTP/TCP transport failure.

Collection Interval: 5 min

Peg Condition: Pegged when a connection is closed without the peer sending a DPR.

Measurement Scope: Server Group

Recovery:

1. If this measurement indicates an excessive number of ungraceful peer disconnects the Alarm History should be examined to determine the reason for the peer disconnects.
2. Contact the *Customer Care Center* for assistance if needed.

RxConnDupPkts

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of duplicate packets received on the TCP connection.

Collection Interval: 5 min

Peg Condition: When duplicate packet is received on the TCP connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnDupTsns

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of duplicate TSNs received on the SCTP connection.

Collection Interval: 5 min

Peg Condition: When there is a duplicate TSN received on the SCTP connection from the remote peer.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnGapAckBlocks

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of gap acknowledgement blocks received on the SCTP connection.

Collection Interval: 5 min

Peg Condition: When there is a gap in the Peer's received subsequences of data chunks as represented by their Transport Sequence Numbers (TSNs).

Measurement Scope: Server Group

Recovery:

No action required.

TxConnRetransDataChunks

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of retransmitted data chunks sent on the SCTP connection.

Collection Interval: 5 min

Peg Condition: When a data chunk is retransmitted on the SCTP connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnRetransSegs

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of retransmit segments sent on the TCP connection.

Collection Interval: 5 min

Peg Condition: When a retransmitted segment is sent on the TCP connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnSendFail

Measurement Group: Connection Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the transport send failed for any message on an established connection. When this occurs, the transport connection will NOT be disconnected.

Collection Interval: 5 min

Peg Condition: Pegged when the DSR is unable to send a message on the connection

Measurement Scope: Server Group

Recovery:

1. If this measurement indicates an excessive number of send failures, examine the *TxConnSendBufPeak* and *TxConnSendBufAvg* measurements.
2. Contact the *Customer Care Center* for assistance if needed.

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.

Table 40: Connection Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvConnCnxSuccess	Number of times the transport connection was successfully established. In instances where two connections are established and one is disconnected after an election, both connection establishments are counted.	5 min
EvPerConnQueueCongestionChange	Number of times that the congestion level changed for a Connection.	5 min

Measurement Tag	Description	Collection Interval
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.	5 min
RxConnMsgs	Number of messages received on the connection. This includes all Diameter messages, both routable and non-routable.	5 min
RxConnOctets	Number of octets received on the connection. This includes Diameter payload octets for all Diameter messages, both routable and non-routable.	5 min
RxConnPeakMPS	Peak rate of the exponentially smoothed average rate in MPS on the connection	5 min
RxConnRecvBufAvg	Average number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.	5 min
RxConnRecvBufPeak	Peak number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.	5 min
RxMsgRateAvg	Average Connection Ingress Message Rate.	5 min
RxMsgRatePeak	Peak Connection Ingress Message Rate.	5 min
RxSctpChunkMp	Number of SCTP data chunks received by the MP (excluding duplicates).	5 min
RxSctpPacketMp	Number of SCTP packets received by the MP (excluding duplicates).	5 min
TmRxMPSDelay_MaxCapacity	Total amount of time during the measurement reporting interval that the connection experienced	5 min

Measurement Tag	Description	Collection Interval
	delay in ingress message processing because the ingress message rate on the connection exceeded the connection's configured Maximum Ingress MPS	
TmRxMPSDelay_SharedCapacity	Total amount of time during the measurement reporting interval that the connection experienced delay in ingress message processing due to no capacity available in the MP server's shared ingress MPS pool	5 min
TxConnMsgs	Number of messages sent on the connection. This includes all Diameter messages, both routable and non-routable.	5 min
TxConnOctets	Number of octets sent on the connection. This includes Diameter payload octets for all Diameter messages, both routable and non-routable.	5 min
TxConnSendBufAvg	Average number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.	5 min
TxConnSendBufPeak	Peak number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.	5 min
TxConnTotalDataChunks	|The number of total data chunks sent on the SCTP connection.	5 min
TxPerConnQueueAvg	Per Connection Egress Message Queue Average Utilization.	5 min

Measurement Tag	Description	Collection Interval
TxPerConnQueuePeak	Per Connection Egress Message Queue Peak Utilization.	5 min

EvConnCnxSuccess

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the transport connection was successfully established. In instances where two connections are established and one is disconnected after an election, both connection establishments are counted.

Collection Interval: 5 min

Peg Condition: Pegged when a socket connection is made, regardless of which side initiates the connection.

Measurement Scope: Server Group

Recovery:

No action required.

EvPerConnQueueCongestionChange

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times that the congestion level changed for a Per Connection Egress Queue.

Collection Interval: 5 min

Peg Condition: Each time the congestion level for a Per Connection Egress Queue was changed.

Measurement Scope: Server Group

Recovery:

1. An IP network, or Diameter peer, problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem, preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.

4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the *Customer Care Center*.

RxConnAvgMPS

Measurement Group: Connection Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Connection ID)

Description: 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 KPI.

Collection Interval: 5 min

Peg Condition: This measurement is driven by the SysMetric.

Measurement Scope: Per network, per NE, per MP server

Recovery:

This measurement indicates the exponentially smoothed 30-second average of the ingress messages per second over the measurement reporting interval. The average rate is exponentially smoothed over a 30 second interval to help eliminate variance caused by bursts in the ingress message rate. This measurement, if reported periodically, provides a history of the ingress messaging rate for each connection.

This measurement can also be seen in near real-time by viewing the connection status screen (**Diameter** > **Maintenance** > **Connections**).

No action required.

RxConnMsgs

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of messages received on the connection. This includes all Diameter messages, both routable and non-routable.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnOctets

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of octets received on the connection. This includes Diameter payload octets for all Diameter messages, both routable and non-routable.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnPeakMPS

Measurement Group: Connection Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Connection ID)

Description: Peak rate of the exponentially smoothed average rate in MPS on the connection.

Collection Interval: 5 min

Peg Condition: This measurement is driven by the SysMetric.

Measurement Scope: Per network, per NE, per MP server

Recovery:

This measurement indicates the highest average rate in ingress messages per second that was processed by the Diameter connection. In other words, this measurement shows the highest value of measurement ConnIngressAvgMPS during the measurement reporting interval.

No action required.

RxConnRecvBufAvg

Measurement Group: Connection Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Connection ID)

Description: The average number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.

Collection Interval: 5 min

Peg Condition: Periodically (currently once a second) the depth of the socket receive buffer is measured and the value used to update this measurement.

Measurement Scope: Server Group

Recovery:

1. If this measurement is at or above 80%, this may be an indication that the SCTP/TCP socket receive buffer size is too small, or that the Local Node is unable to handle the load it is presented. Increase the SCTP/TCP Socket Receive Buffer Size from the Connection Configuration Set for this connection.
2. If this does not improve the situation, consider load-sharing with other DSRs.
3. Contact the *Customer Care Center* for assistance if needed.

RxConnRecvBufPeak

Measurement Group: Connection Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Connection ID)

Description: The peak number of bytes in the SCTP/TCP receive buffer. The bytes in the receive buffer are those received from the peer but not yet read by the peer state machine.

Collection Interval: 5 min

Peg Condition: Periodically (currently once a second) the depth of the socket receive buffer is measured and the value used to update this measurement.

Measurement Scope: Server Group

Recovery:

1. If this measurement exceeds the SCTP/TCP socket receive buffer size, this may be an indication that the SCTP/TCP socket receive buffer size is too small, or that the Local Node is unable to handle the load it is presented. Increase the SCTP/TCP Socket Receive Buffer Size from the Connection Configuration Set for this connection.
2. If this does not improve the situation, consider load-sharing with other DSRs.
3. Contact the *Customer Care Center* for assistance if needed.

RxMsgRateAvg

Measurement Group: Connection Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Connection ID)

Description: The average connection ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).

Collection Interval: 5 min

Peg Condition: The average of all connection ingress message rate samples taken during the collection interval.

The connection measurement is associated with the connection from which the 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

RxMsgRatePeak

Measurement Group: Connection Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Connection ID)

Description: The peak connection ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).

Collection Interval: 5 min

Peg Condition: The maximum connection ingress message rate (messages per second) sample taken during the collection interval.

The connection measurement is associated with the connection from which the 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

TmRxMPSDelay_MaxCapacity

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time in milliseconds that the connection experienced delay in ingress message processing because the ingress message rate on the connection exceeded the connection's configured Maximum Ingress MPS.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by the denial read delay in milliseconds each time a capacity refresh request results in no additional capacity due to the connection's maximum ingress MPS budget being exhausted.

Measurement Scope: Per network, per NE, per MP server

Recovery:

Consistently high values in this measurement indicate that the ingress message rate on the Diameter connection may be higher than the maximum ingress MPS value the connection was configured with. When this measurement is incremented, it indicates that the per connection ingress MPS control feature is throttling its rate of reading messages from the connection.

This measurement is not intended to measure how much delay is being introduced into the connection's ingress message processing; rather it is intended to give a general idea of how often per connection ingress MPS control throttling is occurring due to exhaustion of the connection's maximum ingress MPS capacity.

Note: This measurement may also be incremented due to normal spikes in the ingress MPS rate. Therefore occasional non-zero values or low values should not cause concern. If the ingress MPS rate is truly too high, Alarm *22328 - Connection is processing a higher than normal ingress messaging rate* should also be present for the connection.

No action required.

TmRxMPSDelay_SharedCapacity

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: Total amount of time in milliseconds that the connection experienced delay in ingress message processing due to no capacity available in the DA MP's Shared Pool.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by the denial read delay in milliseconds each time a capacity refresh request results in no additional capacity due to lack of shared ingress MPS capacity on the MP server that hosts the connection.

Measurement Scope: Per network, per NE, per MP server

Recovery:

Consistent non-zero values in this measurement indicate that the connection was delayed in reading a message because there was no available shared ingress MPS capacity remaining on the MP server. Connections use shared ingress MPS capacity when their maximum ingress MPS is configure higher than their reserved ingress MPS and the actual rage of ingress traffic is higher than the reserved ingress MPS value. When connections competing for shared ingress MPS capacity exhaust the MP server's licensed capacity, the per connection ingress MPS control feature delays the connection trying to read an ingress message. When this occurs, this measurement is incremented.

When this measurement is non-zero for connections using shared capacity, it indicates that the MP server is processing ingress messaging rates near or exceeding its licensed capacity. If this measurement is only rarely non-zero, the delays are in response to spikes in the ingress messaging rate. This latter condition can generally be ignored.

This measurement is not intended to measure how much delay is being introduced into the connection's ingress message processing; rather it is intended to give a general idea of how often per connection ingress MPS control throttling is occurring due to exhaustion of the MP server's shared ingress MPS capacity.

Please look for alarm-id 22328 to determine if any one connection is using capacity well above its configured maximum ingress MPS rate. Note, however, that it is possible for all connections to be operating within their configured maximum ingress MPS rates, but the sum of those rates exceeds the MP servers licensed MPS capacity.

No action required.

TXConnMsgs

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of messages sent on the connection. This includes all Diameter messages, both routable and non-routable.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is sent to the peer on the connection

Measurement Scope: Server Group

Recovery:

No action required.

TxConnOctets

Measurement Group: Connection Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of octets sent on the connection. This includes all Diameter messages, both routable and non-routable.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is sent to the peer on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnSendBufAvg

Measurement Group: Connection Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Connection ID)

Description: The average number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.

Collection Interval: 5 min

Peg Condition: Periodically (currently once a second) the depth of the socket send buffer is measured and the value used to update this measurement.

Measurement Scope: Server Group

Recovery:

1. If this measurement is at or above 80%, this may be an indication that the peer is unable to handle the load it is presented with. Consider load-sharing with other Peer Nodes.
2. Contact the *Customer Care Center* for assistance if needed.

TxConnSendBufPeak

Measurement Group: Connection Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Connection ID)

Description: The peak number of bytes in the SCTP/TCP send buffer. The SCTP/TCP send buffer contains all bytes sent to the SCTP/TCP socket by the peer state machine which have not yet been sent to the peer or have been sent to the peer and have not been unacknowledged.

Collection Interval: 5 min

Peg Condition: Periodically (currently once a second) the depth of the socket send buffer is measured and the value used to update this measurement.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnTotalDataChunks

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:

No action required.

TxPerConnQueueAvg

Measurement Group: Connection Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Connection ID)

Description: The average Per Connection Egress Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all Per Connection Egress Message Queue utilization samples taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.

4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the *Customer Care Center*.

TxPerConnQueuePeak

Measurement Group: Connection Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Connection ID)

Description: The peak Per Connection Egress Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum Per Connection Egress Message Queue utilization sample taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the *Customer Care Center*.

Diameter Signaling Router (DSR) Application Exception measurements

The "DSR Application Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the DSR protocol.

Table 41: DSR Application Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxApplRequestNoRoutes	Number of Request messages received from a DSR Application that could not be routed.	5 min
RxApplUnavailable	Number of Request messages received for a DSR Application that could not be routed to the DSR Application because it was Unavailable.	5 min
RxApplUnavailableForRequest	Number of Request messages received for a DSR Application which could not be routed to DSR Application because it was not available.	5 min
RxApplUnavailableForAnswer	Number of Answer messages received for a DSR Application which could not be routed to DSR Application because it was not available.	5 min
TxCpaFullDRLAnswerReject	The number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.	5 min
TxCpaFullDRLRequestReject	The number of egress Diameter Request messages that were rejected because the DRL's Request Queue was full.	5 min
TxFabrFullDRLRequestReject	The average Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
TxFabrFullDRLAnswerDiscard	The number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.	5 min
TxRbarFullDRLRequestReject	Egress Request Messages Rejected - DRL Request Queue Full.	5 min
TxRbarFullDRLAnswerDiscard	Egress Answer Messages Discarded - DRL Answer Queue Full.	5 min
TxGlaFullDRLAnswerDiscard	The number of egress Diameter Answer messages that were	5 min

Measurement Tag	Description	Collection Interval
	discarded because the DRL's Answer Queue was full.	

RxApplRequestNoRoutes

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Request messages received from a DSR Application that could not be routed.

Collection Interval: 5 min

Peg Condition: When DRL successfully receives a Request message from s DSR Application that is rejected with an Answer response because either a Peer Routing Rule was not found or implicit routing could not be invoked.

Measurement Scope: Server Group

Recovery:

The DSR Application is forwarding Request messages that cannot be routed to a peer. The following problems could exist:

- A Peer Routing Rule could be missing of incorrectly configured.
- The DSR Application could be incorrectly configured.
- The Request message from a downstream peer was mis-routed to the DSR.

1. Verify the Peer Routing Rules on the following GUI screen, and make any needed corrections.
   Diameter>Configuration>Peer Routing Rules
2. Verify the DSR Application Id configuration on the following GUI screen, and make any needed corrections.
   Diameter>Configuration>Application Ids

RxApplUnavailable

Measurement Group: DSR Application Exception

Measurement Type: Simple

Description: Number of Request messages received for a DSR Application that could not be routed to the DSR Application because the DSR Application was Unavailable.

Collection Interval: 5 min

Peg Condition: When DRL receives a Request message from a peer that matches an Application Routing Rule, but cannot be routed to the DSR Application because its Operational Status is "Unavailable".

Measurement Scope: Server Group

Recovery:

The DSR Application Operational Status is "Unavailable" when one of the following conditions occurs:

- The operator has removed the DSR Application from service (Admin State is "Disabled".)
- The DSR Application was congested when an attempt to route a Request message to the SR Application occurred.

When a DSR Application is "Unavailable", the message will be handled as defined by the "unavailability Action" attribute for the DSR Application (see the GUI screen for the DSR Application).

1. Verify the DSR Application Admin State on the following GUI screen:
   Diameter>Maintenance>Applications
2. Verify the DSR Application "Unavailability Action" attribute configuration on the following GUI screen..
   Diameter>Configuration>Application Ids

RxApplUnavailableForAnswer

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Answer messages received for a DSR Application which could not be routed to DSR Application because it was not available.

Collection Interval: 5 min

Peg Condition: When DRL receives an Answer message from a peer associated with a PTR indicating that the Answer response must be routed back to the DSR Application but cannot be routed to the DSR Application because its Operational Status is “Unavailable.”

Measurement Scope: Server Group

Recovery:

A DSR Application’s Operational Status is “Unavailable” when one of the following conditions occur:

- The operator has removed the DSR Application from service (Admin State is “Disabled”)
- The DSR Application was congested when an attempt to route a Request message to the DSR Application occurred.

When a DSR Application is "Unavailable", the message will be handled as defined by the "unavailability Action" attribute for the DSR Application (see the GUI screen for the DSR Application).

1. Verify the DSR Application Admin State on the following GUI screen:
   Diameter>Maintenance>Applications
2. Verify the DSR Application "Unavailability Action" attribute configuration on the following GUI screen..
   Diameter>Configuration>Application Ids

RxApplUnavailableForRequest

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Request messages received for a DSR Application which could not be routed to DSR Application because it was not available.

Collection Interval: 5 min

Peg Condition: When DRL receives a Request message from a peer which matches a ART rule but cannot be routed to the DSR Application because its Operational Status was not “Available”.

Measurement Scope: Server Group

Recovery:

A DSR Application’s Operational Status is “Unavailable” when one of the following conditions occur:

- The operator has removed the DSR Application from service (Admin State is “Disabled”)
- The DSR Application was congested when an attempt to route a Request message to the DSR Application occurred.

When a DSR Application is "Unavailable", the message will be handled as defined by the "unavailability Action" attribute for the DSR Application (see the GUI screen for the DSR Application).

1. Verify the DSR Application Admin State on the following GUI screen:

   Diameter>Maintenance>Applications

2. Verify the DSR Application "Unavailability Action" attribute configuration on the following GUI screen..

   Diameter>Configuration>Application Ids

TxCpaFullDRLRequestReject

Measurement Group: DSR Application Exception

Measurement Type: Average

Measurement Dimension: Single

Description: The number of egress Diameter Request messages that were rejected because the DRL’s Request Queue was full.

Collection Interval: 5 min

Peg Condition: For each Request message discarded because the “DRL’s Request Queue” was full. Used for congestion control by DSR.

Measurement Scope: Server Group

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.

- 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.
- If the problem persists, contact the *Customer Care Center*.

TxCpaFullDRLAnswerDiscard

Measurement Group: DSR Application Exception

Measurement Type: Average

Measurement Dimension: Single

Description: The number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.

Collection Interval: 5 min

Peg Condition: For each Answer message discarded because the "All-Connections Event Queue" was full. Used for congestion control by DSR.

Measurement Scope: Server Group

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.
- 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.
- If the problem persists, contact the *Customer Care Center*.

TxFabrFullDRLRequestReject

Measurement Group: DSR Application Exception

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:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.
- 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.
- If the problem persists, contact the *Customer Care Center*.

TxFabrFullDRLAnswerDiscard

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.

Collection Interval: 5 min

Peg Condition: For each Answer message discarded because the "All-Connections Event Queue" was full.

Measurement Scope: Server Group

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.
- 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.
- If the problem persists, contact the *Customer Care Center*.

TxRbarFullDRLRequestReject

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of egress Diameter Request messages that were rejected because the DRL's Request Queue was full.

Collection Interval: 5 min

Peg Condition: When a Request message is discarded because the DRL's Request Queue is full.

Measurement Scope: Server Group

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.
- 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.
- If the problem persists, contact the *Customer Care Center*.

TxRbarFullDRLAnswerDiscard

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.

Collection Interval: 5 min

Peg Condition: When an Answer message is discarded because the All-Connections Event Queue is full.

Measurement Scope: Server Group

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.
- 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.
- If the problem persists, contact the *Customer Care Center*.

TxGlaFullDRLAnswerDiscard

Measurement Group: DSR Application Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of egress Diameter Answer messages that were discarded because the DRL's Answer Queue was full.

Collection Interval: 5 min

Peg Condition: Each time an Answer message is discarded because the "All-Connections Event Queue" was full.

Measurement Scope: Server Group

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional Message Processor (MP) processing capacity at a Network Element and indicates overall MP congestion is occurring.

- 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.
- 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.
- If the problem persists, contact the *Customer Care Center*.

Diameter Signaling Router (DSR) Application Performance measurements

The "DSR Application Performance" measurement group is a set of measurements that provide performance information that is specific to the DSR protocol. These measurements will allow the user to determine how many messages are successfully forwarded and received to and from each DSR Application.

Table 42: DSR Application Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxApplAnswerFwdSuccess	Number of Answer messages successfully forwarded to a DSR Application	5 min
RxApplAnswerReceived	Number of Answer messages received from a DSR Application	5 min
RxApplRequestFwdSuccess	Number of Request messages successfully forwarded to a DSR Application	5 min
RxApplRequestReceived	Number of Request messages received from a DSR Application	5 min
RxCpaAnswerMsgQueueAvg	The average Answer Message Queue utilization (0-100%)	5 min

Measurement Tag	Description	Collection Interval
	measured during the collection interval.	
RxCpaAnswerMsgQueuePeak	The peak Answer Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxCpaAnswerProcessed	The total number of Answers processed by DSR Application.	5 min
RxCpaEventMsgQueueAvg	The average CPA Application Event Message Queue utilization measured during the collection interval.	5 min
RxCpaEventMsgQueuePeak	The peak CPA Application Event Message Queue utilization measured during the collection interval.	5 min
RxCpaMsgRateAvg	The average DSR Application's Message Processing rate measured during the collection interval.	5 min
RxCpaMsgRatePeak	The peak DSR Application's Message Processing rate measured during the collection interval.	5 min
RxCpaRequestMsgQueueAvg	The average Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxCpaRequestMsgQueuePeak	The peak DSR Application's Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxCpaRequestProcessed	The total number of Requests processed by DSR Application.	5 min
RxFabrMsgRateAvg	The average DSR Application's Ingress Message Rate measured during the collection interval.	5 min
RxFabrMsgRatePeak	The peak DSR Application's Ingress Message Rate measured during the collection interval.	5 min
RxFabrRequestMsgQueueAvg	The average Request Message Queue utilization (0-100%)	5 min

Measurement Tag	Description	Collection Interval
	measured during the collection interval.	
RxFabrRequestMsgQueuePeak	The peak DSR Application's Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxGlaRequestMsgQueuePeak	The peak DSR Application's Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxGlaRequestMsgQueueAvg	The average Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxGlaMsgRatePeak	The peak DSR Application's Ingress Message Rate measured during the collection interval.	5 min
RxGlaMsgRateAvg	The average DSR Application's Ingress Message Rate measured during the collection interval.	5 min
RxGlaRequestProcessed	The number of Requests processed by a DSR Application during the collection interval.	5 min
RxFabrRequestProcessed	The number of Requests processed by a DSR Application during the collection interval.	5 min
RxRbarMsgRateAvg	DSR Application Message Processing Rate	5 min
RxRbarMsgRatePeak	DSR Application Message Processing Rate Peak	5 min
RxRbarRequestMsgQueueAvg	DSR Application Request Message Queue Average Utilization	5 min
RxRbarRequestMsgQueuePeak	DSR Application Request Message Queue Peak Utilization	5 min
RxRbarRequestProcessed	Total number of Requests processed by DSR Application	5 min
TxApplTransSuccess	Number of Transactions initiated by DSR Application that successfully completed	5 min

RxApplAnswerFwdSuccess

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Answer messages successfully forwarded to a DSR Application.

Collection Interval: 5 min

Peg Condition: When DRL successfully enqueues an Answer message on the DSR Application's internal Message Queue.

Measurement Scope: Server Group

Recovery:

No action required.

RxApplAnswerReceived

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Request messages received from a DSR Application.

Collection Interval: 5 min

Peg Condition: When DRL successfully receives a Request message from a DSR Application.

Measurement Scope: Server Group

Recovery:

No action required.

RxApplRequestFwdSuccess

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Request messages successfully forwarded to a DSR Application.

Collection Interval: 5 min

Peg Condition: When DRL successfully enqueues a Request message on the DSR Application's internal Message Queue.

Measurement Scope: Server Group

Recovery:

No action required.

RxApplRequestReceived

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Request messages received from a DSR Application.

Collection Interval: 5 min

Peg Condition: When DRL successfully receives a Request message from a DSR Application.

Measurement Scope: Server Group

Recovery:

No action required.

RxCpaAnswerMsgQueueAvg

Measurement Group: DSR Application 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:

No action required.

RxCpaAnswerMsgQueuePeak

Measurement Group: DSR Application 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:

No action required.

RxCpaAnswerProcessed

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of Answers processed by DSR Application.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when a Diameter Answer is received.

Measurement Scope: Server Group

Recovery:

No action required.

RxCpaEventMsgQueueAvg

Measurement Group: DSR Application Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average CPA Application Event Message Queue utilization measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average Event Message Queue utilization sample taken during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaEventMsgQueuePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak CPA Application Event Message Queue utilization measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum Event Message Queue utilization sample taken during the collection interval.

Measurement Scope: Network, NE, Server Group

Recovery:

No action required.

RxCpaMsgRateAvg

Measurement Group: DSR Application Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average DSR Application's Message Processing rate measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all message processing rate samples taken during the collection interval. Used for congestion control by DSR.

Measurement Scope: Server Group

Recovery:

No action required.

RxCpaMsgRatePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak DSR Application's Message Processing rate measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum message processing rate sample taken during the collection interval. Used for congestion control by DSR.

Measurement Scope: Server Group

Recovery:

No action required.

RxCpaRequestMsgQueueAvg

Measurement Group: DSR Application 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:

No action required.

RxCpaRequestMsgQueuePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak DSR Application's 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:

No action required.

RxCpaRequestProcessed

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of Requests processed by DSR Application.

Collection Interval: 5 min

Peg Condition: This measurement will be incremented when a Diameter Request is received.

Measurement Scope: Server Group

Recovery:

No action required.

RxFabrMsgRateAvg

Measurement Group: DSR Application Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average DSR Application's Ingress Message Rate measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all DSR Application Ingress Message Rate samples taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Verify the configuration using **Diameter** > **Configuration** > **Application Routing Rules**.

   The Application Routing Table may be mis-configured and sending too much traffic to the DSR Application.

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

   The MPs may be unable to handle the network load. MPs are in a congestion state when the ingress message rate to the MP is exceeding its capacity to process the messages.

3. If the problem persists, contact the *Customer Care Center*.

RxFabrMsgRatePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak DSR Application's Ingress Message Rate measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum DSR Application Ingress Message Rate sample taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Verify the configuration using **Diameter** > **Configuration** > **Application Routing Rules**.

   The Application Routing Table may be mis-configured and sending too much traffic to the DSR Application.

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

   The MPs may be unable to handle the network load. MPs are in a congestion state when the ingress message rate to the MP is exceeding its capacity to process the messages.

3. If the problem persists, contact the *Customer Care Center*.

RxFabrRequestMsgQueueAvg

Measurement Group: DSR Application 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. Display and monitor the DSR Application status by selecting **Diameter>Maintenance>Applications**. Verify that the Admin State is set as expected.

   The DSR Application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.
2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter>Configuration >Application Routing Rules**.
3. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Request Message Queue. Examine the Alarm log in **Alarms & Events**
4. If the problem persists, contact the *Customer Care Center*.

RxFabrRequestMsgQueuePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak DSR Application’s 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. Display and monitor the DSR Application status by selecting **Diameter>Maintenance>Applications**. Verify that the Admin State is set as expected.

The DSR Application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.

2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter>Configuration >Application Routing Rules**.
3. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Request Message Queue. Examine the Alarm log in **Alarms & Events**
4. If the problem persists, contact the *Customer Care Center*.

RxFabrRequestProcessed

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Requests processed by a DSR Application during the collection interval.

Collection Interval: 5 min

Peg Condition: For each Request message successfully de-queued from the DSR Application's Request Message queue.

Measurement Scope: Server Group

Recovery:

No action required.

RxGlaMsgRateAvg

Measurement Group: DSR Application Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average DSR Application's Ingress Message Rate measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all DSR Application Ingress Message Rate samples taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: **Diameter** > **Configuration** > **Application Routing Rules**
2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored from Main Menu: **Status & Manage** > **KPIs**. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

3. Contact the *Customer Care Center* for further assistance.

RxGlaMsgRatePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak DSR Application's Ingress Message Rate measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum DSR Application Ingress Message Rate sample taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: **Diameter** > **Configuration** > **Application Routing Rules**
2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored from Main Menu: **Status & Manage** > **KPIs**. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. Contact the *Customer Care Center* for further assistance.

RxGlaRequestMsgQueueAvg

Measurement Group: DSR Application 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. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: **Diameter** > **Configuration** > **Application Routing Rules**
2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored from Main Menu: **Status & Manage** > **KPIs**. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. Contact the *Customer Care Center* for further assistance.

RxGlaRequestMsgQueuePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak DSR Application's 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. Determine if the Application Routing Table is mis-configured and sending too much traffic to the DSR Application. Verify the configuration via the Main Menu: **Diameter** > **Configuration** > **Application Routing Rules**
2. Determine if there are an insufficient number of MPs configured to handle the network load. The ingress traffic rate of each MP can be monitored from Main Menu: **Status & Manage** > **KPIs**. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. Contact the *Customer Care Center* for further assistance.

RxGlaRequestProcessed

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Requests processed by a DSR Application during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time a Request message successfully de-queued from the DSR Application's Request Message queue.

Measurement Scope: Server Group

Recovery:

No action required.

RxRbarMsgRateAvg

Measurement Group: DSR Application Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average DSR Application's Ingress Message Rate measured during the collection interval

Collection Interval: 5 min

Peg Condition: When the average of all DSR Application Ingress Message Rate samples is taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Display and monitor the DSR Application message rate by selecting **Diameter** > **Maintenance** > **Applications**. Verify that the message rate is set as expected.
2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
3. There might be an insufficient number of MPs configured to handle the network load. Monitor the traffic rate of each MP by selecting **Diameter** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, contact the *Customer Care Center*.

RxRbarMsgRatePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Peak DSR Application's Ingress Message Rate measured during the collection interval

Collection Interval: 5 min

Peg Condition: When the maximum DSR Application Ingress Message Rate sample is taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Display and monitor the DSR Application message rate by selecting **Diameter** > **Maintenance** > **Applications**. Verify that the message rate is set as expected.
2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
3. There might be an insufficient number of MPs configured to handle the network load. Monitor the traffic rate of each MP by selecting **Diameter** > **Status & Manage** > **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, contact the *Customer Care Center*.

RxRbarRequestMsgQueueAvg

Measurement Group: DSR Application Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average Request Message Queue utilization (0-100%) measured during the collection interval

Collection Interval: 5 min

Peg Condition: When the average of all Request Message Queue utilization samples is taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications**. Verify that the Operational Reason, which indicates congestion level, is set as expected.

   The DSR Application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.
2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
3. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Request Message Queue. Examine the Alarm log in **Alarms & Events**
4. If the problem persists, contact the *Customer Care Center*.

RxRbarRequestMsgQueuePeak

Measurement Group: DSR Application Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Peak DSR Application's Request Message Queue utilization (0-100%) measured during the collection interval

Collection Interval: 5 min

Peg Condition: When the maximum Request Message Queue utilization sample is taken during the collection interval.

Measurement Scope: Server Group

Recovery:

1. Display and monitor the DSR Application status by selecting **Diameter** > **Maintenance** > **Applications**. Verify that the Operational Reason, which indicates congestion level, is set as expected.

   The DSR Application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.
2. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Routing Rules**.
3. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its Request Message Queue. Examine the Alarm log in **Alarms & Events**
4. If the problem persists, contact the *Customer Care Center*.

RxRbarRequestProcessed

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Requests processed by a DSR Application during the collection interval

Collection Interval: 5 min

Peg Condition: When a Request message is successfully de-queued from the DSR Application's Request Message queue.

Measurement Scope: Server Group

Recovery:

No action required.

TxApplTransSuccess

Measurement Group: DSR Application Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by DSR Application ID)

Description: Number of Request messages received from a DSR Application.

Collection Interval: 5 min

Peg Condition: When DRL successfully receives a Request message from a DSR Application.

Measurement Scope: Server Group

Recovery:

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.

Table 43: Diameter Egress Transaction Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxAnswerExpectedAll	Number of valid Answer messages received from an upstream peer that were associated with a pending transaction.	5 min

Measurement Tag	Description	Collection Interval
RxAnswerMsgQueueFullDiscard	The number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.	5 min
TxAnswerTimeout	Number of times that an Answer response was not received from a peer before the maximum allowed time PENDING_ANSWER_TIMER.	5 min
TxConnAnswerMsgs	Number of routable Answer messages successfully sent on the connection.	5 min
TxConnectionFailed	Egress peer-to-peer transactions aborted by a Local Node - connection failure.	5 min
TxConnRequestMsgs	Number of routable Request messages successfully sent on the connection.	5 min
TxRequestSuccessAllConn	Number of Request messages successfully routed to a peer.	5 min

RxAnswerExpectedAll

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:

No action required.

RxAnswerMsgQueueFullDiscard

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. Contact the *Customer Care Center* for assistance if needed.

TxAnswerTimeout

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 PENDING-ANSWER-TIMER.

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. Contact the *Customer Care Center* for assistance if needed.

TxConnAnswerMsgs

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:

No action required.

TxConnectionFailed

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. Contact the *Customer Care Center* for assistance if needed.

TxConnRequestMsgs

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:

No action required.

TxRequestSuccessAllConn

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:

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.

Table 44: Diameter Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvApplIdListInconsistency	Number of times that the supported Application IDs received from the Peer were Inconsistent with another Transport Connection	5 min
EvConnCeaIdValFail	Number of times the connection was closed due to CEA Realm/Host validation for locally initiated connections. **Note:** CER Realm/Host validation failures are tracked via the EvConnCerIdValFail measurement and are NOT included in this measurement.	5 min

Measurement Tag	Description	Collection Interval
EvConnCexTO	Number of times the connection timed out waiting for the peer to send a CER or CEA.	5 min
EvConnDpaTO	Number of times the connection timed out waiting for the peer to send a DPA.	5 min
EvConnNoComnApps	Number of times the connection was closed due to there being no common application IDs existing between the local and peer nodes.	5 min
EvConnPrvFail	Number of times the connection was closed after failing to successfully complete the proving phase.	5 min
EvConnRejected	Number of times the connection was rejected. Reasons include IP addresss validation failure, the connection already established, and connection Administratively Disabled.	5 min
EvConnRejInsufficientIngressMps	Number of times DA-MP rejected a Diameter connection due to insufficient Ingress MPS on the DA-MP to support the Reserved Ingress MPS configured for the connection.	5 min
EvConnRejMaxConnExceeded	Number of times DA-MP rejected a Diameter connection due to the DA-MP exceeding its maximum number of supported Diameter connections.	5 min
EvConnWdFail	Number of times the Diameter Watchdog algorithm closed the connection due to no traffic received from the peer within Tw*2 time after a DWR was sent.	5 min
EvConnWdSuspect	Number of times the Diameter Watchdog algorithm declared the connection suspect due to no traffic received from the peer within Tw time after a DWR was sent.	5 min

Measurement Tag	Description	Collection Interval
EvMpCerIdValFail	Number of times the connection was closed due to CER Realm/Host validation for peer initiated connections.	5 min
EvTransLifetimeExceededMp	Number of transaction failures because "Transaction Lifetime" exceeded.	5 min
RxAnswerMsgQueueFullDiscard	Number of ingress Diameter Answer messages that were discarded because the Answer Message Queue was full.	5 min
RxAnswerUnexpected	Number of valid Answer messages received from an upstream peer that could not be associated with a pending transaction	5 min
RxConnCeaError	Number of CEA error messages received on the connection.	5 min
RxConnFailMalfMsg	Number of messages received on the connection which were malformed. Malformed messages cause the connection to be closed.	5 min
RxConnInvalidMsg	Number of messages received on the connection which had a semantic error. Messages with semantic errors are discarded.	5 min
RxConnMpCongestionAnswerRsp	Number of ingress messages that were rejected with an error response because of local congestion.	5 min
RxConnUnexpCex	Number of unexpected CER/CEA messages received on the connection.	5 min
RxConnUnexpDpx	Number of unexpected DPR/DPA messages received on the connection.	5 min
RxConnUnexpDwx	Number of unexpected DWR/DWA messages received on the connection.	5 min
RxMaxMpsAnswerRsp	The number of ingress Diameter messages that were discarded because of the MP Maximum	5 min

Measurement Tag	Description	Collection Interval
	MPS limitation and an Answer response was sent.	
RxMaxMpsRejectMp	The number of ingress Diameter messages that were rejected because of MP Maximum MPS limitation and an Answer response was sent.	5 min
RxMpCongestionDiscardMp	The number of ingress Diameter Request messages received that were discarded or rejected because of local MP congestion.	5 min
RxMpCongestionRejectMp	The number of ingress Diameter messages that were discarded because of Local MP Congestion and an Answer response was sent.	5 min
RxMsgsOCGreenPri0DiscardMp	The number of Green ingress Priority 0 messages discarded by the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri0DiscardMp	The number of Yellow ingress Priority 0 messages discarded by the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri1DiscardMp	The number of Green ingress Priority 1 messages discarded by the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri1DiscardMp	The number of Yellow ingress Priority 1 messages discarded by the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri2DiscardMp	The number of Green ingress Priority 2 messages discarded by the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri2DiscardMp	The number of Yellow ingress Priority 2 messages discarded by the DA-MP Overload Control component.	5 min
RxPduPoolEmptyDiscard	The number of Diameter messages that were discarded because no PDU Buffers were available.	5 min

Measurement Tag	Description	Collection Interval
RxRoutableRejectMsgsMp	The number of ingress Diameter Request messages received that are rejected by MP with Error Answer due to MP Overload Control or Maximum IMR Limitation.	5 min
TmConnDegraded	Total time (in seconds) during the reporting period that the connection state was in the Degraded state.	5 min
TmConnEnabledNotAvail	Total time (in seconds) during the reporting period that the connection state was Administratively Enabled and the connection state was not Available.	5 min
TxAllConnQueueFullAnswerDiscard	The number of egress Diameter Answer messages that were discarded because the All-Connections Event Queue was full and an Answer response was sent.	5 min
TxAllConnQueueFullDiscard	Number of egress Diameter messages that were discarded because the All-Connections Event Queue was full.	5 min
TxConnCeaError	Number of CEA error messages sent on the connection.	5 min
TxConnUnavailDiscard	Number of egress Diameter messages that were discarded by DCL because the egress connection was Unavailable.	5 min
TxReqMsgApplMismatch	Number of times message routing detected application mismatch	5 min
TxReqMsgPerConnPtrMax	Number of times message routing bypassed the connection because the maximum allowed pending transactions was exceeded	5 min
TxRequestEgressLoop	Outgoing message loops detected	5 min

EvApplIdListInconsistency

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, contact the *Customer Care Center*.

EvConnCeaIdValFail

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the connection was closed due to CEA Realm/Host validation for locally initiated connections.

Collection Interval: 5 min

Peg Condition: Pegged when a CEA message is received on the connection that has an Origin-Host AVP value that does not match the FQDN configured for the peer, or an Origin-Realm AVP value that does not match the realm configured for the peer.

Measurement Scope: Server Group

Recovery:

1. Examine the Origin-Host and Origin-Realm AVP values in the CEA sent by the peer.
2. Either change the FQDN/Realm configured for the peer to match this value, or change the peer so that it sends Origin-Host/Origin-Realm AVP values that match the peer FQDN/Realm configuration.
3. Contact the *Customer Care Center* for assistance if needed.

EvConnCexTO

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the connection timed out waiting for the peer to send a CEx.

Collection Interval: 5 min

Peg Condition: Pegged when a peer initiated a connection and fails to send a CER within Tcex (from the Connection Configuration Set) seconds of the socket connection being established, or when the DSR initiates a connection and the peer fails to send a CEA within Tcex (from the Connection Configuration Set) seconds of the DSR sending a CER.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it did not send the appropriate CEx message.
2. Contact the *Customer Care Center* for assistance if needed.

EvConnDpaTO

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection timed out waiting for the peer to send a DPA.

Collection Interval: 5 min

Peg Condition: Pegged when a peer fails to send a DPA within Tdpx (from the Connection Configuration Set) seconds of the DSR sending a DPR.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it did not respond to the DPR message that the DSR sent to it.
2. Contact the *Customer Care Center* for assistance if needed.

EvConnNoComnApps

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection was closed due to there being no common Application IDs existing between the Local and Peer Nodes.

Collection Interval: 5 min

Peg Condition: Pegged when a CEx message is received on the connection that has

1. No Application IDs specified (when in Relay mode), or
2. No Application IDs in common with those configured for the local node or
3. If any of the Application IDs marked as 'MUST exist in Peer CEx', in the CEx Cfg Set of that connection object, is not present in the CEx message

Measurement Scope: Server Group

Recovery:

Verify that either the Auth-Application-ID, the Acct-Application-ID, or the Vendor-Specific-Application-ID AVPs are present in the CEx message sent by the peer.

EvConnPrvFail

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the connection was closed after failing to successfully complete the proving phase.

Collection Interval: 5 min

Peg Condition: Pegged when a peer fails a proving period.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it did not respond in a timely fashion to the DWRs sent during the proving period.
2. Consider increasing the Proving Timer in the Connection Configuration Set for the connection to allow more time for the peer to respond to DWRs.
3. Contact the *Customer Care Center* for assistance if needed.

EvConnRejected

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection was rejected. Reasons include IP address validation failure, the connection already established, and connection administratively disabled.

Collection Interval: 5 min

Peg Condition: Pegged when a connection is rejected for any reason.

Measurement Scope: Server Group

Recovery:

1. Examine the Alarm History to determine the specific reason(s) for the connection being rejected.
2. Contact the *Customer Care Center* for assistance if needed.

EvConnRejInsufficientIngressMps

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The sum of the Reserved Ingress MPS for the added connection and MP Reserved Ingress MPS has exceeded the MP Maximum Reserved Ingress MPS. The number of times DA-MP rejected a Diameter connection due to insufficient Ingress MPS on the DA-MP to support the Reserved Ingress MPS configured for the connection.

Collection Interval: 5 min

Peg Condition: This measurement is incremented for each Diameter connection that was rejected.

Measurement Scope: Server Group

Recovery:

1. The value for Reserved Ingress MPS for the added connection needs to be examined to determine if its value should be decreased.
2. Contact the *Customer Care Center* for assistance.

EvConnRejMaxConnExceeded

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The maximum number of active Diameter connections supported by a DA-MP has been exceeded. The number of times DA-MP rejected a Diameter connection due to the DA-MP exceeding its maximum number of supported Diameter connections.

Collection Interval: 5 min

Peg Condition: This measurement is incremented for each Diameter connection that is rejected by a DA-MP.

Measurement Scope: Server Group

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 the *Customer Care Center*.

EvConnWdFail

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the Diameter watchdog algorithm closed the connection due to no traffic received from the peer within Tw*2 seconds after a DWR was sent.

Collection Interval: 5 min

Peg Condition: Pegged when no messages were received from the peer within Tw*2 seconds of sending a DWR to the peer.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it is not responding to requests.
2. Contact the *Customer Care Center* for assistance if needed.

EvConnWdSuspect

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times the Diameter watchdog algorithm declared the connection suspect due to no traffic received from the peer within Tw seconds after a DWR was sent.

Collection Interval: 5 min

Peg Condition: Pegged when no Diameter messages are received on the connection for Tw seconds after a DWR was sent to the peer.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it is not responding to requests.
2. Contact the *Customer Care Center* for assistance if needed.

EvMpCerIDValFail

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times the connection was closed due to CER Realm/Host validation for peer initiated connections.

Collection Interval: 5 min

Peg Condition: Pegged when the value Origin-Host and/or Origin-Realm AVPs sent by the peer in its CER message do not match the values provisioned for the connection.

Measurement Scope: Server Group

Recovery:

1. Examine the Alarm History to determine the Origin Host and Realm sent by the peer.
2. Compare these values to those configured in the Peer Node object for this connection. These values must match in order for the peer connection to be validated.
3. Contact the *Customer Care Center* for assistance if needed.

EvTransLifetimeExceededMp

Measurement Group: DSR Application 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:

No action required.

RxAnswerMsgQueueFullDiscard

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. Contact the *Customer Care Center* for assistance if needed.

RxAnswerUnexpected

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 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:

No action required.

RxConnCeaError

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of CEA error messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a CEA message with a non-success response code is received on the connection.

Measurement Scope: Server Group

Recovery:

1. Examine the Alarm History to determine why the connection is being rejected.
2. Contact the *Customer Care Center* for assistance if needed.

RxConnFailMalfMsg

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of messages received on the connection which were malformed. Malformed messages cause the connection to be closed.

Collection Interval: 5 min

Peg Condition: Pegged when a message is received on the connection that cannot be decoded.

Measurement Scope: Server Group

Recovery:

1. Examine the Alarm History and find event *22302 - Connection Unavailable: Received malformed message* for this connection.
2. Examine the displayed message bytes for errors. Monitor the connection for invalid Diameter messages.
3. Contact the *Customer Care Center* for assistance if needed.

RxConnInvalidMsg

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of messages received on the connection which had a semantic error. Messages with semantic errors are discarded.

Collection Interval: 5 min

Peg Condition: Pegged when a message is received on the connection that cannot be decoded.

Measurement Scope: Server Group

Recovery:

1. Examine the Alarm History and find event *22311 - Invalid Diameter message received* for this connection.
2. Examine the displayed message bytes for errors.
3. Contact the *Customer Care Center* for assistance if needed.

RxConnMpCongestionAnswerRsp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of ingress messages that were rejected with an error response because of local congestion.

Collection Interval: 5 min

Peg Condition: For each ingress Diameter message that was rejected because of local MP congestion and an Answer response was sent.

The connection measurement is associated with the connection from which the 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

RxConnUnexpCex

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of unexpected CER/CEA messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a CER/CEA message is received on the connection after the capabilities exchange has been completed. Pegged when a CER is expected from the peer and a CEA received, or vice versa.

Measurement Scope: Server Group

Recovery:

1. Examine the Alarm History and find event *22308 - Received Unexpected CER/CEA* for this connection to determine the reason that the CEx was unexpected.
2. Contact the *Customer Care Center* for assistance if needed.

RxConnUnexpDpx

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of unexpected DPR/DPA messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DPx message is received on the connection before the capabilities exchange has been completed, or when a DPA is received without a DPR being sent to it.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it is sending non-CEx messages before the capabilities exchange is complete, or why it is sending a DPA without receiving a DPR.
2. Contact the *Customer Care Center* for assistance if needed.

RxConnUnexpDwx

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of unexpected DWR/DWA messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DWx message is received on the connection before the capabilities exchange has been completed.

Measurement Scope: Server Group

Recovery:

1. Examine the peer to determine why it is sending non-CEx messages before the capabilities exchange is complete.
2. Contact the *Customer Care Center* for assistance if needed.

RxDOCRejectConn

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of ingress messages that were discarded because of local DA-MP danger of CPU congestion.

Collection Interval: 5 min

Peg Condition: For each message discarded on a connection due to DA-MP danger of CPU congestion.

The connection measurement is associated with the connection from which the message was received.

Measurement Scope: Server Group

Recovery:

1. The 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. 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, contact the *Customer Care Center*.

RxDOCRejectConn

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of ingress Diameter messages that were rejected with an error response because of local DA-MP danger of CPU congestion.

Collection Interval: 5 min

Peg Condition: For each message discarded on a connection with a DIAMETER (Error) Answer due to DA-MP danger of CPU congestion.

The connection measurement is associated with the connection from which the message was received.

Measurement Scope: Server Group

Recovery:

1. The 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. 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, contact the *Customer Care Center*.

RxDOCRejectMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter 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 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. 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, contact the *Customer Care Center*.

RxMpCongestionDiscardMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages received that were discarded or rejected because of local MP congestion.

Collection Interval: 5 min

Peg Condition: For each ingress Diameter Request message discarded because of local MP 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. 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 the *Customer Care Center*.

RxMpCongestionRejectMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Description: The number of ingress messages that were rejected with error answer due to local DA-MP CPU congestion

Collection Interval: 5 min

Peg Condition: Pegged for each message discarded with a DIAMETER (Error) Answer due to a DA-MP 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. 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 the *Customer Care Center*.

RxMsgsOCGreenPri0DiscardMp

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

RxMsgsOCYellowPri0DiscardMp

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

RxMsgsOCGreenPri1DiscardMp

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

RxMsgsOCYellowPri1DiscardMp

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

RxMsgsOCGreenPri2DiscardMp

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

RxMsgsOCYellowPri2DiscardMp

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

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

RxPduPoolEmptyDiscard

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Diameter messages that were discarded because no PDU buffers were available.

Collection Interval: 5 min

Peg Condition: For each Diameter message discarded.

The connection measurement is associated with the connection the message was received from.

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. Contact the *Customer Care Center* for assistance if needed.

RxRoutableRejectMsgsMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages received that are rejected by MP with Error Answer due to MP Overload Control or Maximum IMR Limitation.

Collection Interval: 5 min

Peg Condition: Pegged for each Request message that is rejected.

Measurement Scope: Server Group

Recovery:

1. The 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. Contact the *Customer Care Center* for assistance.
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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, contact the *Customer Care Center*.

TmConnDegraded

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. Contact the *Customer Care Center* for assistance if needed.

TmConnEnabledNotAvail

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. Contact the *Customer Care Center* for assistance if needed.

TxAllConnQueueFullDiscard

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of egress Diameter messages that were discarded because the All-Connections Event Queue was full.

Collection Interval: 5 min

Peg Condition: For each message discarded because the "All-Connections Event Queue" was full

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. If the problem persists, contact the *Customer Care Center*.

TxConnCeaError

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of CEA error messages sent on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a CEA message with a non-success response code is sent on the connection.

Measurement Scope: Server Group

Recovery:

1. Examine the alarm history to determine why the connection is being rejected.
2. Contact the *Customer Care Center* for assistance if needed.

TxConnUnavailDiscard

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of egress Diameter messages that were discarded by DCL because the egress connection was Unavailable.

Collection Interval: 5 min

Peg Condition: For each egress message discarded because the egress connection was found to be Unavailable.

Measurement Scope: Server Group

Recovery:

No action required.

TxReqMsgApplMismatch

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of times a selected egress peer was not selected because it does not support the target Application ID in the message header.

Collection Interval: 5 min

Peg Condition: Each time the DSR bypasses a transport connection during route selection because the Application ID in the Request message does not match one of the Application IDs received from the peer on the transport connection during the Diameter Capabilities Exchange procedure.

The connection measurement is associated with the egress connection to which an Application ID was not supported for routing the message.

Measurement Scope: Server Group

Recovery:

Contact the *Customer Care Center* for assistance if needed.

TxReqMsgPerConnPtrMax

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, contact the *Customer Care Center*.

TxRequestEgressLoop

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:

Contact the *Customer Care Center* 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.

Table 45: Diameter Ingress Transaction Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxAnsFwdFailed	The number of times an ingress Diameter Answer message could not be forwarded to the appropriate	5 min

Measurement Tag	Description	Collection Interval
	DA-MP, because the DA-MP was unavailable or congested.	
RxDecodeFailure	Number of Request messages rejected from a downstream peer because the message could not be decoded.	5 min
RxDiscardedMsgsPerConnControlsMp	Total number of ingress Diameter messages, over all connections, that were discarded by this MP. Discard is either due to the connection exceeding its configured maximum capacity, or unavailable shared capacity.	5 min
RxMaxMpsDiscardConn	Number of ingress Diameter Request messages received on a connection that were discarded because of MP Maximum MPS limitation.	5 min
RxMaxMpsDiscardMp	The number of ingress Diameter Request messages received on a connection that were discarded because of Local MP Congestion without Error Answer.	5 min
RxMessageLooping	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).	5 min
RxMpCongestionDiscard	Number of ingress Diameter Request messages received on a connection that were discarded because of local MP congestion.	5 min
RxNoRoutesFound	Number of Request messages from a downstream peer rejected by a Local Node because no routes were available for routing the message.	5 min
RxNoRulesFailure	Number of Request messages from a downstream peer rejected by a Local Node because no Peer Routing Rule was found.	5 min

Measurement Tag	Description	Collection Interval
RxPrtRuleRejection	Number of Request messages from a downstream peer rejected by a Local Node because a peer routing rule ACTION is set to "Send Answer".	5 min
RxRejectedAll	Number of Request messages rejected from a downstream peer by a Local Node (all reasons).	5 min
RxRejectedOther	Number of Request messages from a downstream peer rejected by a Local Node for any reason other than those identified by other measurements.	5 min
RxRequestMsgQueueFullDiscard	Number of ingress Diameter Request messages that were discarded because the Request Message Queue was full.	5 min
RxRoutableDiscardedMsgsMp	The number of ingress Diameter Request messages received that are discarded by MP without Error Answer due to MP Overload Control or Maximum IMR Limitation.	5 min
RxTransactionTimeout	Number of Request messages from a downstream peer rejected by a Local Node because maximum message reroutes exceeded.	5 min
TxLongTimeoutPtrListEmpty	Number of ingress Diameter Request messages that were discarded because no Long Timeout PTR Buffers were available.	5 min
TxPerConnQueueFullDiscard	Number of egress messages that were discarded because the "Per Connection Egress Message Queue" was full.	5 min
TxPerConnQueueFullAnswerDiscard	Number of egress Answer messages that were discarded because the Per Connection Egress Message Queue was full.	5 min
TxPerConnQueueFullRequestDiscard	Number of egress Request messages that were discarded because the Per Connection Egress Message Queue was full.	5 min

Measurement Tag	Description	Collection Interval
TxPtrPoolEmpty	Number of ingress Diameter Request messages that were discarded because no PTR Buffers were available.	5 min
TxRerouteQueueFullReject	Number of egress Diameter Request messages that were rejected because the Reroute Queue was full.	5 min
TxSockFullDiscard	Number of egress Diameter messages that were discarded because the socket was not writable.	5 min

RxAnsFwdFailed

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times an ingress Diameter Answer message could not be forwarded to the appropriate DA-MP, because the DA-MP was unavailable or congested.

Collection Interval: 5 min

Peg Condition: This peg is incremented when a DA-MP receives a Diameter Answer message, identifies the DA-MP that holds the pending transaction, however finds that the DA-MP is unavailable or congested.

Measurement Scope: Server Group

Recovery:

If this measurement is seen to be incrementing consistently, contact the *Customer Care Center*.

This measurement should be pegged, only when the DSR process on the destination DA-MP is Unavailable or the DA-MP is rebooting.

RxDecodeFailure

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. Contact the *Customer Care Center* for assistance if needed.

RxDiscardedMsgsPerConnControlsMp

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of ingress Diameter messages, over all connections, that were discarded by this MP. Discard is either due to the connection exceeding its configured maximum capacity, or unavailable shared capacity.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message, received on any peer connection, is discarded due to exceeding the configured maximum ingress MPS.

Measurement Scope: Server Group

Recovery:

No action required.

RxMpCongestionDiscardConn

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of ingress messages that were discarded because of local DA-MP CPU congestion.

Collection Interval: 5 min

Peg Condition: For each message discarded on a connection due to a DA-MP CPU congestion.

The connection measurement is associated with the connection from which the message was received.

Measurement Scope: Server Group

Recovery:

1. The 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. 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, contact the *Customer Care Center*.

RxDOCDiscardMp

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages received on a connection 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. 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 the *Customer Care Center*.

RxMessageLooping

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, contact the *Customer Care Center*.

RxMpCongestionDiscardConn

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of ingress Diameter Request messages received on a connection that were discarded because of local MP congestion without Error Answer.

Collection Interval: 5 min

Peg Condition: For each ingress Diameter Request message discarded because of local MP congestion.

The connection measurement is associated with the connection from which the 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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

RxNoRoutesFound

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. Contact the *Customer Care Center* 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. Contact the *Customer Care Center* for assistance if needed.

RxNoRulesFailure

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).

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, contact the *Customer Care Center*.

RxPrtRuleRejection

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.

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.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope: Server Group

Recovery:

No action required.

RxRejectedAll

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 ID *RxRejectedConnCongestion*, *RxDecodeFailure*, *RxMessageLooping*, *RxConnInvalidMsg*, *RxNoRulesFailure*, *RxNoRoutesFound*, *RxTransactionTimeout*, *RxPrtRuleRejection*, or *RxRejectedOther* is pegged.

Measurement Scope: Server Group

Recovery:

No action required.

RxRejectedOther

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*, *RxConnInvalidMsg*, *RxNoRulesFailure*, *RxNoRoutesFound*, *RxTransactionTimeout*, 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*, *RxConnInvalidMsg*, *RxNoRulesFailure*, *RxNoRoutesFound*, *RxTransactionTimeout*, or *RxPrtRuleRejection*.

The connection measurement is associated with the connection from which the Request message was received.

Measurement Scope: Server Group

Recovery:

No action required.

RxRequestMsgQueueFullDiscard

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. Contact the *Customer Care Center* for assistance if needed.

RxRoutableDiscardedMsgsMp

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages received that are discarded by MP without Error Answer due to MP Overload Control or Maximum IMR Limitation.

Collection Interval: 5 min

Peg Condition: Pegged when Diameter Request message is discarded.

Measurement Scope: Server Group

Recovery:

1. The 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. Contact the *Customer Care Center* for assistance.
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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
6. If the problem persists, contact the *Customer Care Center*.

RxTransactionTimeout

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. Contact the *Customer Care Center* for assistance if needed.

TxLongTimeoutPtrListEmpty

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Single

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, contact the *Customer Care Center*.

TxPerConnQueueFullDiscard

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of egress messages that were discarded because the "Per Connection Egress Message Queue" was full.

Collection Interval: 5 min

Peg Condition: For each message discarded because the "Per Connection Egress Message Queue" was full

Measurement Scope: Server Group

Recovery:

1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. Examine the alarm log from **Main Menu** > **Alarms & Events**.

3. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
4. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. 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
6. If the problem persists, contact the *Customer Care Center*.

TxPerConnQueueFullAnswerDiscard

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of egress Answer messages that were discarded because the Per Connection Egress Message Queue was full.

Collection Interval: 5 min

Peg Condition: For each Per Connection Egress Message Queue Answer message discarded.

Measurement Scope: Server Group

Recovery:

1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the *Customer Care Center*.

TxPerConnQueueFullRequestDiscard

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of egress Request messages that were discarded because the Per Connection Egress Message Queue was full.

Collection Interval: 5 min

Peg Condition: For each Per Connection Egress Message Queue Request message discarded.

Measurement Scope: Server Group

Recovery:

1. An IP network or Diameter peer problem may exist that is preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. The alarm log should be examined using the **Alarms & Events** page.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. MP server status can be monitored using the **Status & Manage** > **Server** page.
4. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored using the **Status & Manage** > **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
6. If the problem persists, contact the *Customer Care Center*.

TxPtrListEmpty

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. Contact the *Customer Care Center* for assistance if needed.

TxRerouteQueueFullReject

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. Contact the *Customer Care Center* for assistance if needed.

TxSockFullDiscard

Measurement Group: Diameter Ingress Transaction Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of egress Diameter messages that were discarded because the socket was not writable.

Collection Interval: 5 min

Peg Condition: For each egress Diameter message discarded because the socket was not writable.

Measurement Scope: Server Group

Recovery:

1. An IP network or Diameter peer problem may exist thus preventing SCTP/TCP from transmitting messages into the network at the same pace that messages are being received from the network.
2. The transport task associated with the connection may be experiencing a problem preventing it from processing events from its Connection Event Message Queue. Examine the alarm log from **Main Menu** > **Alarms & Events**.
3. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
4. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Main Menu** > **Status & Manage** > **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. 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
6. If the problem persists, contact the *Customer Care Center*.

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.

Table 46: Diameter Ingress Transaction Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxConnRequestMsgs	Number of routable Request messages received on the connection	5 min
TxAnswer1xxx	Ingress Answer messages from peers successfully routed - Result-Code value 1xxx (Informational)	5 min
TxAnswer2xxx	Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 2xxx (Success)	5 min
TxAnswer3xxx	Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 3xxx (Protocol Error)	5 min
TxAnswer4xxx	Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 4xxx (Transient Failure)	5 min

Measurement Tag	Description	Collection Interval
TxAnswer5xxx	Answer messages from upstream peers successfully routed to downstream peers - Result-Code value 5xxx (Permanent Failure)	5 min
TxAnswerFailure	Expected Answer responses from a peer or Answer responses created by a Local Node which were not successfully routed to a downstream peer (for any reason).	5 min
TxAnswerLocalNode	Answer messages created by Local Node successfully routed to downstream peers (all Result-Code values)	5 min
TxAnswerOther	Answer messages from upstream peers successfully routed to downstream peers - Result-Code value not 1000-5999	5 min

RxConnRequestMsgs

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:

No action required.

TxAnswer1xxx

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 DSR 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:

No action required.

TxAnswer2xxx

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 DSR 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:

No action required.

TxAnswer3xxx

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 DSR 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:

No action required.

TxAnswer4xxx

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 DSR 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:

No action required.

TxAnswer5xxx

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 DSR 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:

No action required.

TxAnswerFailure

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 DSR 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:

No action required.

TxAnswerLocalNode

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 DSR 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:

No action required.

TxAnswerOther

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 DSR 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:

No action required.

Diameter Performance measurements

The Diameter Performance measurement report contains measurements that provide performance information that is specific to the Diameter protocol.

Table 47: Diameter Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvConnPrvSuccess	Number of times the connection successfully completed the proving phase.	5 min
EvPerConnPtrQueueAvg	The average length of the PTR queue for a connection during the collection interval.	5 min
EvPerConnPtrQueuePeak	The maximum length of the PTR queue for a connection during the collection interval	5 min
RoutingMsgs	The number of messages processed by DRL , including Rerouting and Message Copy.	5 min
RxAcceptedRequestsMp	The number of ingress Diameter Request messages that are accepted by MP to be routed after all Overload Controls are applied.	5 min
RxAllowedMsgsPerConnControlsMp	The total number of ingress Diameter messages, over all connections, that were not discarded by MP.	5 min
RxAnswerExpectedAll	Number of valid Answer messages received from an upstream peer that were associated with a pending transaction.	5 min
RxAnswerExpectedAllMp	Number of valid Answer messages received from an upstream peer that were associated with a pending transaction.	5 min
RxAnswerExpectedRoutedMP	Number of valid Answer messages received from an upstream peer that	5 min

Measurement Tag	Description	Collection Interval
	were successfully routed to a downstream peer.	
RxAnswerMsgsMp	Number of Answer messages received.	5 min
RxConnAnswerMsgs	Number of routable Answer messages received on the connection.	5 min
RxConnCea	Number of CEA messages received on the connection.	5 min
RxConnCer	Number of CER messages received on the connection.	5 min
RxConnDpa	Number of DPA messages received on the connection.	5 min
RxConnDpr	Number of DPR messages received on the connection	5 min
RxConnDwa	Number of DWA messages received on the connection.	5 min
RxConnDwr	Number of DWR messages received on the connection.	5 min
RxConnOtherNonRoutable	Number of non-routable messages received on the connection that were not CEx, DWx, or DPx messages. Includes messages where the header P(roxy) bit is not set and messages where the application ID is 0.	5 min
RxConnRequestMsgs	Number of routable Request messages received on the connection.	5 min
RxConnRoutableMsgs	Number of routable messages received on the connection.	5 min
RxMaxMpsAcceptedMp	The number of ingress Diameter messages received that are accepted by Maximum IMR Controls of MP.	5 min
RxMaxMpsAcceptedRequestsMp	The number of ingress Diameter Request messages that are accepted by MP to be routed after Maximum IMR Controls are applied by MP.	5 min
RxMsgSize	Ingress message size statistics.	5 min
RxMsgSizeAvg	Average ingress message size in Diameter payload octets.	5 min

Measurement Tag	Description	Collection Interval
RxMsgSizePeak	Peak ingress message size in Diameter payload octets.	5 min
RxMsgsOCPri0Mp	The number of ingress Priority 0 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri0Mp	The number of Green ingress Priority 0 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri0Mp	The number of Yellow ingress Priority 0 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri1Mp	The number of ingress Priority 1 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri1Mp	The number of Green ingress Priority 1 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri1Mp	The number of Yellow ingress Priority 1 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri2Mp	The number of ingress Priority 2 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri2Mp	The number of Green ingress Priority 2 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri2Mp	The number of Yellow ingress Priority 2 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri3Mp	The number of ingress Priority 3 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri0RatePeakMp	The peak rate of ingress Priority 0 messages arriving at the DA-MP Overload Control component.	5 min

Measurement Tag	Description	Collection Interval
RxMsgsOCGreenPri0RatePeakMp	The peak rate of Green ingress Priority 0 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri0RatePeakMp	The peak rate of Yellow ingress Priority 0 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri1RatePeakMp	The peak rate of ingress Priority 1 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri1RatePeakMp	The peak rate of Green ingress Priority 1 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri1RatePeakMp	The peak rate of Yellow ingress Priority 1 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri2RatePeakMp	The peak rate of ingress Priority 2 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCGreenPri2RatePeakMp	The peak rate of Green ingress Priority 2 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCYellowPri2RatePeakMp	The peak rate of Yellow ingress Priority 2 messages arriving at the DA-MP Overload Control component.	5 min
RxMsgsOCPri3RatePeakMp	The peak rate of ingress Priority 3 messages arriving at the DA-MP Overload Control component.	5 min
RxOfferedMsgsMp	Total number of ingress Diameter messages, over all connections, offered to this MP. This includes both routable and non-routable messages.	5 min
RxRequestMsgsMp	Number of Request messages received.	5 min
RxRequestNoErrors	Transactions successfully processed on one routing attempt.	5 min

Measurement Tag	Description	Collection Interval
RxRequestNoErrorsMp	Number of transactions successfully processed on one routing attempt.	5 min
RxRoutableAcceptedMsgsMpmn	The number of ingress Diameter messages received that are accepted by MP for processing after all overload controls are applied.	5 min
RxRoutableMsgsMp	Number of routable messages received.	5 min
TmConnAvail	Total time in seconds that the connection state was AVAILABLE during the measurement period.	5 min
TmConnPrvRspAvg	Average time (in microseconds) between sending a DWR and receiving a DWA during any proving phase(s) for the measurement period. If proving fails, no sample is recorded.	5 min
TmResponseTimeDownstream	Average downstream transaction response time.	5 min
TmResponseTimeDownstreamMp	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.	5 min
TmResponseTimeUpstream	Average upstream transaction response time.	5 min
TxAnswerMsgsMp	Number of routable Answer messages transmitted.	5 min
TxConnAnswerMsgs	Number of routable Answer messages successfully sent on the connection.	5 min
TxConnCea	Number of CEA messages sent on the connection.	5 min
TxConnCer	Number of CER messages received on the connection.	5 min
TxConnDpa	Number of DPA messages sent on the connection.	5 min
TxConnDpr	Number of DPR messages sent on the connection.	5 min

Measurement Tag	Description	Collection Interval
TxConnDwa	Number of DWA messages sent on the connection.	5 min
TxConnDwr	Number of DWR messages received on the connection.	5 min
TxConnRequestMsgs	Number of routable Request messages successfully sent on the connection.	5 min
TxMsgSize	Average egress message size in Diameter payload octets.	5 min
TxMsgSizeAvg	Average egress message size in Diameter payload octets.	5 min
TxMsgSizePeak	Peak egress message size in Diameter payload octets.	5 min
TxRequestMsgsMp	Number of routable Request messages transmitted.	5 min
TxRequestSuccessAllMp	Number of Request messages successfully routed to a peer.	5 min.

EvConnPrvSuccess

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Connection ID)

Description: The number of times the connection successfully completed the proving phase.

Collection Interval: 5 min

Peg Condition: Pegged when a proving period is successfully completed.

Measurement Scope: Server Group

Recovery:

1. If the proving mode in the Connection Configuration Set is set to On Error, and this measurement indicates an excessive number of proving periods being performed, examine measurements *TxConnDpr*, *RxConnDpa*, *RxConnDpr*, and *TxConnDpa*.
2. Also examine the Alarm History for events *22303 - Connection Unavailable: Peer closed connection*, *22319 - Connection Unavailable: Diameter Watchdog* and *22345 - Connection Priority Level changed*.

   The presence of these measurements/events may indicate that the peer is not responding to DWRs or not handling the DPx exchange on disconnect properly, after which the DSR will require a proving period.
3. Contact the *Customer Care Center* for assistance if needed.

EvPerConnPtrQueueAvg

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:

No action required.

EvPerConnPtrQueuePeak

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:

No action required.

RoutingMsgs

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of messages processed by DRL, including Rerouting and Message Copy.

Collection Interval: 5 min

Peg Condition: This peg should be incremented per any of these conditions.

- Ingress Request processing resulting in the Request being routed upstream (with or without local DSR application processing of the Request)

- Ingress Answer processing resulting in forwarding of Answer downstream (with or without local DSR application processing of the Answer)
- Ingress Request processing resulting in Answer message sent by DSR to originator (with or without local DSR application processing of the Request)
- Ingress Request discarded due to validation error or overload
- Ingress Answer discarded due to validation error
- Initial copy and transmit of a Request to a DAS
- Ingress Answer triggering reroute of the pending Request message (including Answers from DAS for copied Requests)
- 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 Request copy completion or termination

Measurement Scope: Server Group

Recovery:

No action necessary.

RxAcceptedRequestsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages that are accepted by MP to be routed after all Overload Controls are applied.

Collection Interval: 5 min

Peg Condition: For each message forwarded to DRl for routing

Measurement Scope: Server Group

Recovery:

No action required.

RxAcceptedMsgsPerConnControlsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of ingress Diameter messages, over all connections, that were not discarded by MP

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message, received on any peer connection, is not discarded due to not exceeding the configured maximum ingress MPS.

Measurement Scope Server Group

Recovery:

No action required.

RxAnswerExpectedAll

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:

No action required.

RxAnswerExpectedAllMp

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:

No action required.

RxAnswerExpectedRoutedMp

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:

No action required.

RxAnswerMsgsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Answer messages received.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnAnswerMsgs

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of routable Answer messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter answer message is received from the peer.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnCea

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of CEA messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a CEA message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnCer

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of CER messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a CER message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnDpa

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DPA messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DPA message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnDpr

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DPR messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DPR message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnDwa

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DWA messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DWA message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnDwr

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DWR messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DWR message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxConnOtherNonRoutable

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of non-routable messages received on the connection that were not CEx, DWx, or DPx messages. Includes messages where the header Proxy bit is not set and messages where the application ID is 0.

Collection Interval: 5 min

Peg Condition: Pegged when a message is received with the Proxy bit not set and the Application ID is 0, and the command code is not CEx, DWx, or DPx.

Note: If this measurement is non-zero, the peer is sending commands to be processed by the Local Node that the Local Node does not understand. These messages will be discarded.

Measurement Scope: Server Group

Recovery:

1. Monitor the connection to determine which messages are being addressed to the Local Node.
2. Contact the *Customer Care Center* for assistance if needed.

RxConnRequestMsgs

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:

No action required.

RxConnRoutableMsgs

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of routable messages received on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a message with the Proxy bit set is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxMaxMpsAcceptedMp

Measurement Group: Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter messages received that are accepted by Maximum IMR Controls of MP.

Collection Interval: 5 min

Peg Condition: Pegged for each message not discarded or rejected with "Discard Message" or "Drop Message & Send Response".

Measurement Scope: Server Group

Recovery:

No action required.

RxMaxMpsAcceptedRequestsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter Request messages that are accepted by MP to be routed after Maximum IMR Controls are applied by MP.

Collection Interval: 5 min

Peg Condition: Each time a Diameter Request message is not discarded or rejected

Measurement Scope: Server Group

Recovery:

No action required.

RxMsgSize

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Ingress message size statistics.

Note: Each bucket in the array contains the number of PDUs with Diameter payload octets that fell within the bucket's range during the measurement period.

- [0] = less than 512 octets
- [1] = 512 to 1023 octets
- [2] = 1024 to1535 octets
- [3] = 1536 to 2047 octets
- [4] = 2048 to 2559 octets
- [5] = 2560 to 3071 octets
- [6] = 3072 to 3583 octets
- [7] = 3584 to 4095 octets
- [8] = 4096 or more octets

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

No action required.

RxMsgSizeAvg

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The average ingress message size in Diameter payload octets.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

No action required.

RxMsgSizePeak

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The peak ingress message size in Diameter payload octets.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received from the peer on the connection. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

1. If this measurement exceeds the configured maximum Diameter message size, examine the *RxConnFailMalfMsg* measurement to determine how many messages were discarded because of this condition.
2. Examine the Alarm History and find event *22302 - Connection Unavailable: Received malformed message* for this connection.
3. Examine the displayed message bytes for errors and monitor the connection for invalid Diameter messages.
4. Contact the *Customer Care Center* for assistance if needed.

RxMsgsOCPri0Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Priority 0 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 0 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCGreenPri0Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Green ingress Priority 0 messages arriving at 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

Recovery:

No action required

RxMsgsOCYellowPri0Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Yellow ingress Priority 0 messages arriving at 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

Recovery:

No action required

RxMsgsOCPri1Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Priority 1 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 1Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCGreenPri1Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Green ingress Priority 1 messages arriving at 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

Recovery:

No action required

RxMsgsOCYellowPri1Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Yellow ingress Priority 1 messages arriving at 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

Recovery:

No action required

RxMsgsOCPri2Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Priority 2 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 2 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCGreenPri2Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Green ingress Priority 2 messages arriving at 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

Recovery:

No action required

RxMsgsOCYellowPri2Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Yellow ingress Priority 2 messages arriving at 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

Recovery:

No action required

RxMsgsOCPri3Mp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Priority 3 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 3 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCPri0RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of ingress Priority 0 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 0 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCGreenPri0RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of Green ingress Priority 0 messages arriving at 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

Recovery:

No action required

RxMsgsOCYellowPri0RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of Yellow ingress Priority 0 messages arriving at 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

Recovery:

No action required

RxMsgsOCPri1RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of ingress Priority 1 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 1 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCGreenPri1RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of Green ingress Priority 1 messages arriving at 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

Recovery:

No action required

RxMsgsOCYellowPri1RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of Yellow ingress Priority 1 messages arriving at 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

Recovery:

No action required

RxMsgsOCPri2RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of ingress Priority 2 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 2 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxMsgsOCGreenPri2RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of Green ingress Priority 2 messages arriving at 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

Recovery:

No action required

RxMsgsOCYellowPri2RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of Yellow ingress Priority 2 messages arriving at 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

Recovery:

No action required

RxMsgsOCPri3RatePeakMp

Measurement Group: Diameter Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak rate of ingress Priority 3 messages arriving at the DA-MP Overload Control component.

Collection Interval: 5 min

Peg Condition: Each time a Priority 3 Diameter Request message arrives at the DA-MP Overload Control component

Recovery:

No action required

RxOfferedMsgsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total number of ingress Diameter messages, over all connections, offered to this MP. This includes both routable and non-routable messages.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is received on any peer connection.

Measurement Scope: Server Group

Recovery:

No action required.

RxRequestMsgsMp

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:

No action required.

RxRequestNoErrors

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 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:

No action required.

RxRequestNoErrorsMp

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:

No action required.

RxRoutableAcceptedMsgsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ingress Diameter messages received that are accepted by MP for processing after all overload controls are applied.

Collection Interval: 5 min

Peg Condition: Pegged when Diameter message is sent to DRL for routing.

Measurement Scope: Server Group

Recovery:

No action required.

RxRoutableMsgsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of routable messages received.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message, with the Proxy bit set, is received from the peer. This measurement is pegged for all messages accepted for processing, as well as those rejected due to local congestion, MPS limitation, etc.

Measurement Scope: Server Group

Recovery:

No action required.

TmConnAvail

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. Contact the *Customer Care Center* for assistance if needed.

TmConnPrvRspAvg

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The average time (in microseconds) between sending a DWR and receiving a DWA during any proving phase(s) for the measurement period. If proving fails, no sample is recorded.

Collection Interval: 5 min

Peg Condition: Pegged after a proving period completes successfully.

Measurement Scope: Server Group

Recovery:

No action required.

TmResponseTimeDownstream

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 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. 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. Contact the *Customer Care Center* for assistance if needed.

TmResponseTimeDownstreamMp

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:

No action required.

TmResponseTimeUpstream

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 DSR successfully queues a Request message. Time interval for each transaction stops when the DSR 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:

Contact the *Customer Care Center* for assistance if needed.

TxAnswerMsgsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of routable Answer messages transmitted.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter Answer message is sent to the peer on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnAnswerMsgs

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:

No action required.

TxConnCea

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of CEA messages sent on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a CEA message is sent on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnCer

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of CER messages sent on the connection.

Collection Interval: 5 min

Peg Condition: When a CER message is sent to the peer on the connection. This measurement is pegged for CER messages indicating success as well as those indicating an error. A separate measurement (TxConnCerErr) is also pegged if the CER indicates an error.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnDpa

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DPA messages sent on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DPA message is sent on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnDpr

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DPR messages sent on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DPR message is sent on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnDwa

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DWA messages sent on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DWA message is sent on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnDwr

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Connection ID)

Description: The number of DWR messages sent on the connection.

Collection Interval: 5 min

Peg Condition: Pegged when a DWR message is received on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxConnRequestMsgs

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:

No action required.

TxMsgSize

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Egress message size statistics.

Note: Each bucket in the array contains the number of PDUs with Diameter payload octets that fell within the bucket's range during the measurement period.

- [0] = less than 512 octets
- [1] = 512 to 1023 octets
- [2] = 1024 to1535 octets
- [3] = 1536 to 2047 octets
- [4] = 2048 to 2559 octets

- [5] = 2560 to 3071 octets
- [6] = 3072 to 3583 octets
- [7] = 3584 to 4095 octets
- [8] = 4096 or more octets

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is sent to the peer on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxMsgSizeAvg

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The average egress message size in Diameter payload octets.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter message is sent to the peer on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxMsgSizePeak

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The peak egress message size in Diameter payload octets.

Collection Interval: 5 min

Peg Condition: Pegged when the size of the Diameter message sent to the peer is larger than any other message sent to the peer during the reporting interval.

Measurement Scope: Server Group

Recovery:

No action required.

TxRequestMsgsMp

Measurement Group: Diameter Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of routable Request messages transmitted.

Collection Interval: 5 min

Peg Condition: Pegged when a Diameter Request message is sent to the peer on the connection.

Measurement Scope: Server Group

Recovery:

No action required.

TxRequestSuccessAllMp

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:

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.

Table 48: Diameter Rerouting Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxRerouteAnswerRsp	Answer messages received associated with rerouted Request messages	5 min
RxRerouteAnswerRspMp	Number of valid Answer messages received from an upstream peer that were	5 min

Measurement Tag	Description	Collection Interval
	associated with a pending rerouted transaction.	
TxRerouteAnswerResponse	Number of message rerouting attempts triggered by the receipt of an Answer response Result-Code value which is a candidate for message rerouting.	5 min
TxRerouteAnswerTimeout	Rerouting attempts triggered by a timeout on the Answer response.	5 min
TxRerouteAttempts	Total number of message rerouting attempts.	5 min
TxRerouteConnFailure	Rerouting attempts triggered by a connection failure.	5 min
TxRerouteSuccessSent	Message rerouting attempts that were successfully rerouted.	5 min

RxRerouteAnswerRsp

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:

No action required.

RxRerouteAnswerRspMp

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:

No action required.

TxRerouteAnswerResponse

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:

No action required.

TxRerouteAnswerTimeout

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. Contact the *Customer Care Center* for assistance if needed.

TxRerouteAttempts

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 one of the following 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 any of the following measurement IDs are pegged: *TxRerouteConnFailure*, *TxRerouteAnswerTimeout*, *TxRerouteAnswerResponse*.

The connection measurement is associated with the upstream connection from which rerouting was triggered.

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 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. Contact the *Customer Care Center* for assistance if needed.

TxRerouteConnFailure

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. Contact the *Customer Care Center* for assistance if needed.

TxRerouteSuccessSent

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:

No action required.

Egress Throttle Group Performance measurements

The Diameter Egress Throttle Group Performance measurement report contains measurements providing information related to a specific ETG.

Table 49: Diameter Egress Throttle Group Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxEtgMsgsLocal	Number of Messages send to members of ETG. This measurements is not aggregate measurement across all MPs but specific for this MP.	5 min
TxEtgMsgRatePeak	Peak Aggregated ETG Request Message Rate calculation made during the collection interval	5 min
TxEtgMsgRateAvg	Average ETG Request Message Rate calculation made during the collection interval	5 min
EvEtgRateCongestionOnset	Number of times an ETG Message Rate Congestion Level was advanced	5 min

Measurement Tag	Description	Collection Interval
EvEtgRateDiscardPri0	Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited	5 min
EvEtgRateDiscardPri1	Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited	5 min
EvEtgRateDiscardPri2	Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited	5 min
EvEtgPendingTransPeak	Peak pending transactions to members of this ETG during the collection interval	5 min
EvEtgPendingTransAvg	Average Pending transactions to this ETG during the collection interval	5 min
EvEtgPendingTransOnset	Number of times an ETG Pending Transaction Limiting Congestion Level was advanced	5 min
EvEtgPendingTransDiscardPri0	Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited	5 min
EvEtgPendingTransDiscardPri1	Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited	5 min
EvEtgPendingTransDiscardPri2	Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited	5 min

TxEtgMsgsLocal

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of messages (Request or Answer) send on a Connection or a Peer which is part of ETG .

Collection Interval: 5 min

Peg Condition: When DRL successfully queues a message (Request (including Reroutes and MessageCopy) or Answer) to DCL for transmission to Connection or a Peer which is part of ETG. This peg is incremented even if ETG Rate Limiting function is Disabled. This peg is incremented only for "Routable" messages i.e messages terminated in DCL layer (eg CEX, DWX) are not counted.

Measurement Scope: Site

Recovery:

No action required

TxEtgMsgRatePeak

Measurement Group: Egress Throttle Group Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by ETG ID)

Description: Peak Aggregated ETG Message Rate calculation made during the collection interval

Collection Interval: 5 min

Peg Condition: An ETG Message Rate calculation A_t is periodically calculated. If the new A_t exceeds any previous A_{t-k} value for the collection interval, then this measurement will be updated with the new A_t value.

Measurement Scope: Site

Recovery:

No action required

TxEtgMsgRateAvg

Measurement Group: Egress Throttle Group Performance

Measurement Type: Avg

Measurement Dimension: Arrayed (by ETG ID)

Description: Average ETG Message Rate calculation made during the collection interval

Collection Interval: 5 min

Peg Condition: Each time an ETG Message Rate calculation A_t is calculated.

Measurement Scope: Site

Recovery:

No action required

EvEtgRateCongestionOnset

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of times an ETG-RCL was advanced.

Collection Interval: 5 min

Peg Condition: Each time the EMR Congestion Level is advanced

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgRateDiscardPri0

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited.

Collection Interval: 5 min

Peg Condition: Each time that Routing Layer discarded a Priority 0 Request message due to last connection evaluated being ETG Rate Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.

5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgRateDiscardPri1

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited.

Collection Interval: 5 min

Peg Condition: Each time that Routing Layer discarded a Priority 1 Request message due to last connection evaluated being ETG Rate Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgRateDiscardPri2

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETD ID)

Description: Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Rate Limited.

Collection Interval: 5 min

Peg Condition: Each time that Routing Layer discarded a Priority 2 Request message due to last connection evaluated being ETG Rate Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EMR" for the ETG is set sufficiently high.
2. Adjust the EMR onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Adjust the "Smoothing Factor" parameter for the ETG if necessary. Increasing the "Smoothing Factor" value places more weight towards the current EMR over the smoothed EMR. Decreasing the "Smoothing Factor" value places more weight towards the smoothed EMR over the current EMR.
4. Verify the "EMR Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EMR throttling too rapidly.
5. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
6. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgPendingTransPeak

Measurement Group: Egress Throttle Group Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by ETG ID)

Description: Peak pending transactions to members of this ETG during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time a new P_t value exceeds any previous P_{t-k} value.

Measurement Scope: Site

Recovery:

No action required

EvEtgPendingTransAvg

Measurement Group: Egress Throttle Group Performance

Measurement Type: Avg

Measurement Dimension: Arrayed (by ETG ID)

Description: Peak pending transactions to members of this ETG during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time a an ETG Pending Request P_t value is calculated.

Measurement Scope: Site

Recovery:

No action required

EvEtgPendingTransCongestionOnset

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of times an ETG-PCL was advanced.

Collection Interval: 5 min

Peg Condition: Each time the ETG Window Congestion Level is advanced

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgPendingTransDiscardPri0

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of Priority 0 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited

Collection Interval: 5 min

Peg Condition: Each time that Routing Layer discarded a Priority 0 Request message due to last connection evaluated being ETG Pending Transaction Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgPendingTransDiscardPri1

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of Priority 1 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited

Collection Interval: 5 min

Peg Condition: Each time that Routing Layer discarded a Priority 1 Request message due to last connection evaluated being ETG Pending Transaction Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.

5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact the *Customer Care Center*.

EvEtgPendingTransDiscardPri2

Measurement Group: Egress Throttle Group Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by ETG ID)

Description: Number of Priority 2 Request Messages discarded (with or without response) due to last connection evaluated for routing being ETG Pending Transaction Limited

Collection Interval: 5 min

Peg Condition: Each time that Routing Layer discarded a Priority 2 Request message due to last connection evaluated being ETG Pending Transaction Limited

Measurement Scope: Site

Recovery:

1. Verify that the "Maximum EPT" for the ETG is set sufficiently high.
2. Adjust the EPT onset/abatement thresholds if necessary. Setting an abatement threshold too close to its onset threshold may trigger oscillation between higher and lower congestion levels.
3. Verify the "EPT Abatement Timeout" for the ETG is set sufficiently high. Short abatement time periods may result in triggering EPT throttling too rapidly.
4. Determine if other connections (not part of this ETG) to the adjacent Diameter Node are out of service thus causing more traffic to be sent on connections/peers of this ETG than what the adjacent Diameter Node can support on a per-connection basis.
5. Determine if the ETG is over-subscribed from a routing perspective. Any recent changes to DSR routing configurable may have inadvertently diverted more message traffic to connections/peers in this ETG.
6. Determine if the Peer is exhibiting congestion, causing it to either drop the Requests or process them slowly, causing Pending Transactions on DSR to increase and exceed the threshold.
7. If the problem persists, contact the *Customer Care Center*.

Full Address Based Resolution (FABR) Application Exception measurements

The "FABR Application Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events that are specific to the FABR feature.

Table 50: FABR Application Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxFabrBlacklistedImsi	Number of request messages received containing IMSI of a Blacklisted subscriber.	5 min
RxFabrBlacklistedMsisdn	Number of request messages received containing MSISDN of Blacklisted subscriber.	5 min
RxFabrDecodeFailureResol	Number of Request messages rejected due to a message decoding error.	5 min
RxFabrInvalidImsiMcc	Number of times an AVP instance present in a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.	5 min
RxFabrResolFailAll	Total number of Request messages received which did not resolve a Destination address.	5 min
RxFabrResolFailCmdcode	Number of Request messages received with an unknown Command Code.	5 min
RxFabrResolFailImpiMatch	Number of Request messages received for which IMPI was used for Destination address resolution, but no Destination address was found.	5 min
RxFabrResolFailImpuMatch	Number of Request messages received for which IMPU was used for Destination address resolution, but no Destination address was found.	5 min
RxFabrResolFailImsiMatch	Number of Request messages received for which IMSI was used for Destination address resolution, but no Destination address was found.	5 min
RxFabrResolFailMsisdnMatch	Number of Request messages received for which MSISDN was used for Destination address resolution, but no Destination address was found.	5 min

Measurement Tag	Description	Collection Interval
RxFabrResolFailNoAddrAvps	Number of Request messages received without a Routing Entity Address AVP.	5 min
RxFabrResolFailNoValidAddr	Number of Request messages received with at least Routing Entity Address AVP but no valid Routing Entity Addresses were found.	5 min
RxFabrUnkApplId	Number of Request messages rejected due to an unknown Application ID.	5 min
TxFabrDbConFail	Number of database queries failed due to the Communication Agent queue exhaustion.	5 min
TxFabrFwdFail	Number of routing attempt failures due to internal resource exhaustion.	5 min

RxFabrBlacklistedImsi

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: The number of request messages received containing IMSI of a Blacklisted subscriber

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception "BlackListed Subscriber" is invoked

Measurement Scope: Server Group

Recovery:

No action required.

RxFabrBlacklistedMsisdn

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: The number of request messages received containing MSISDN of Blacklisted subscriber

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception "BlackListed Subscriber" is invoked

Measurement Scope: Server Group

Recovery:

1. Validate which User identity address is not blacklisted by using DP configuration.
2. If the problem persists, contact the *Customer Care Center*.

RxFabrDecodeFailureResol

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Request messages rejected due to a message decoding error.

Collection Interval: 5 min

Peg Condition: For each routing exception when the Application ID is not valid or the AVP extends beyond the length of the message indicated by the Message Length parameter in the message header.

Measurement Scope: Server Group

Recovery:

Contact the *Customer Care Center* for assistance.

RxFabrInvalidImsiMcc

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times an AVP instance present in a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.

Collection Interval: 5 min

Peg Condition: Each time a Diameter request message is rejected due to the MCC contained in the decoded IMSI falling within one of the configured Reserved MCC Ranges.

Measurement Scope: Server Group

Recovery:

1. Validate the ranges configured in the Reserved MCC Ranges table.
2. Verify that the MCC portion of the decodable IMSI received by RBAR does not fall within the configured Reserved MCC Ranges.
3. If the problem persists, contact the *Customer Care Center*.

RxFabrResolFailAll

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Total number of Request messages received which did not resolve a Destination address.

Collection Interval: 5 min

Peg Condition: For each Request message which did not resolve to a Destination address.

Measurement Scope: Server Group

Recovery:

1. Validate which destination address is associated with the user identity address by using DP GUI.
2. Contact the *Customer Care Center* for assistance.

RxFabrResolFailCmdcode

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with an unknown Command Code.

Collection Interval: 5 min

Peg Condition: For each routing exception where the (Application ID, Command Code) pair in the incoming Request message is not configured.

Measurement Scope: Server Group

Recovery:

The currently provisioned Diameter Application IDs can be viewed in the FABR Configuration & Maintenance GUI.

Contact the *Customer Care Center* for assistance.

RxFabrResolFailDpCongested

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Database queries that failed to be serviced due DP/ComAgent errors.

Collection Interval: 5 min

Peg Condition: When FABR application received service notification indicating Database (DP) or DB connection (ComAgent) Errors (DP timeout, errors, or ComAgent internal errors) for the sent database query.

Measurement Scope: Server Group

Recovery:

RxFabrResolFailImpiMatch

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received for which IMPI was used for Destination address resolution, but no Destination address was found.

Collection Interval: 5 min

Peg Condition: For each message which did not successfully resolve to a Destination using a Routing Entity Type of IMPI.

Measurement Scope: Server Group

Recovery:

1. Validate which destination address is associated with the user identity address by using DP GUI.
2. Contact the *Customer Care Center* for assistance.

RxFabrResolFailImpuMatch

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received for which IMPU was used for Destination address resolution, but no Destination address was found.

Collection Interval: 5 min

Peg Condition: For each message which did not successfully resolve to a Destination using a Routing Entity Type of IMPU.

Measurement Scope: Server Group

Recovery:

1. Validate which destination address is associated with the user identity address by using DP GUI.
2. Contact the *Customer Care Center* for assistance.

RxFabrResolFailImsiMatch

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received for which IMSI was used for Destination address resolution, but no Destination address was found.

Collection Interval: 5 min

Peg Condition: For each message which did not successfully resolve to a Destination using a Routing Entity Type of IMSI.

Measurement Scope: Server Group

Recovery:

1. Validate which destination address is associated with the user identity address by using DP GUI.
2. Contact the *Customer Care Center* for assistance.

RxFabrResolFailMsisdnMatch

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received for which MSISDN was used for Destination address resolution, but no Destination address was found.

Collection Interval: 5 min

Peg Condition: For each message which did not successfully resolve to a Destination using a Routing Entity Type of MSISDN.

Measurement Scope: Server Group

Recovery:

Validate which destination address is associated with the user identity address by using DP GUI.

Contact the *Customer Care Center* for assistance.

RxFabrResolFailNoAddrAvps

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received without a Routing Entity Address AVP.

Collection Interval: 5 min

Peg Condition: For each routing exception with no valid User Identity address found and the number of AVPs searched for the message was 0.

Measurement Scope: Server Group

Recovery:

If this event is considered abnormal, then use validate which AVPs are configured for routing with the Application ID and Command Code using the FABR GUI screen.

Contact the *Customer Care Center* for assistance.

RxFabrResolFailNoValidAddr

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received with at least Routing Entity Address AVP but no valid Routing Entity Addresses were found.

Collection Interval: 5 min

Peg Condition: For each routing exception with no valid User Identity address found and the number of AVPs searched for the message was greater than 0.

Measurement Scope: Server Group

Recovery:

1. If this event is considered abnormal, then use validate which AVPs are configured for routing with the Application ID and Command Code using the FABR GUI screen.
2. Contact the *Customer Care Center* for assistance.

RxFabrUnkApplId

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Request messages rejected due to an unknown Application ID.

Collection Interval: 5 min

Peg Condition: For each routing exception when the Application ID is not valid.

Measurement Scope: Server Group

Recovery:

1. The currently provisioned Diameter Application IDs can be viewed in the FABR Configuration & Maintenance GUI.
2. The currently provisioned Application Routing Rules can be viewed using **Main Menu** > **Diameter** > **Configuration** > **Application Routing Rules.**
3. Contact the *Customer Care Center* for assistance.

TxFabrDbConFail

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of database queries failed due to the Communication Agent queue exhaustion.

Collection Interval: 5 min

Peg Condition: Each time the application attempts to send DP queries and fails due to Communication Agent queue exhaustion.

Measurement Scope: Server Group

Recovery:

Contact the *Customer Care Center* for assistance.

TxFabrFwdFail

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of routing attempt failures due to internal resource exhaustion.

Collection Interval: 5 min

Peg Condition: Each time the application attempts to enqueue a Request message on the DSR Relay Agent's "Request Message Queue" or enqueue a Answer message on "DRL Answer Queue" and it fails (e.g., queue full).

Measurement Scope: Server Group

Recovery:

Contact the *Customer Care Center* for assistance.

Full Address Based Resolution (FABR) Application Performance measurements

The "FABR Application Performance" measurement group is a set of measurements that provide performance information that is specific to the FABR feature. These measurements will allow you to determine how many messages are successfully forwarded and received to and from the FABR Application.

Table 51: DSR Application Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
FabrAverageQueriesPerBundle	Average number of queries per Bundle sent by FABR	5 min
RxDpResponseTimeAvg	Average time (in milliseconds) it takes to receive a DP response after sending the correlated database query.	5 min
RxFabrAvgMsgSize	Average size of Request message received.	5 min

Measurement Tag	Description	Collection Interval
RxFabrBundledResponseEvents	The number of Bundled Response Events received by FABR.	5 min
RxFabrDpResponseMsgQueueAvg	The average DP Response Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxFabrDpResponseMsgQueuePeak	The peak DSR Application's DP Response Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxFabrMsgs	Number of Request messages received by FABR application.	5 min
RxFabrResolAll	Number of Addresses Successfully Resolved to a Destination	5 min
RxFabrResolAllMp	Number of Addresses Successfully Resolved to a Destination by the MP.	5 min
RxFabrResolImpi	Number of Addresses Successful Resolved with Routing Entity type IMPI.	5 min
RxFabrResolImpu	Number of Addresses Successful Resolved with Routing Entity type IMPU.	5 min
RxFabrResolImsi	Number of Addresses Successful Resolved with Routing Entity type IMSI.	5 min
RxFabrResolMsisdn	Number of Addresses Successful Resolved with Routing Entity type MSISDN.	5 min
RxFabrResolRateAvg	Average Addresses Successfully Resolved per second	5 min
RxFabrResolRatePeak	Peak Addresses Successfully Resolved per second.	5 min
TxFabrAbandonRequest	Number of Request message that are abandoned.	5 min
TxFabrBundledQueryEvents	Number of Bundled Query Events sent to ComAgent.	5 mi

Measurement Tag	Description	Collection Interval
TxFabrFwdDefaultDest	Number of Request message forwarding attempts using a Default Destination.	5 min
TxFabrFwdNochange	Number of Request message forwarding attempts without changing the message.	5 min
TxFabrFwdSuccess	Number of Request messages successfully forwarded (all reasons).	5 min
TxFabrMsgAttempt	Number of Request message forwarding attempts (all reasons).	5 min

FabrAverageQueriesPerBundle

Measurement Group: Full Address Resolution Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average number of queries per Bundle sent by FABR

Collection Interval: 5 min

Peg Condition: When FABR successfully sends a Bundled query event to ComAgent for processing

Measurement Scope: Server Group

Recovery:

No action required.

RxDpResponseTimeAvg

Measurement Group: Full Address Resolution Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average time (in milliseconds) it takes to receive a DP response after sending the correlated database query.

Collection Interval: 5 min

Peg Condition: It is calculated based on the total number of sampled database queries during the collection interval.

Measurement Scope: MP

Recovery:

No action necessary.

RxFabrAvgMsgSize

Measurement Group: Full Address Resolution Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Average size of Request message received.

Collection Interval: 5 min

Peg Condition: Average calculated for each Request message received.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrBundledResponseEvents

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Bundled Response Events received by FABR.

Collection Interval: 5 min

Peg Condition: When FABR successfully receives a Bundled response event from ComAgent.

Measurement Scope: Server Group

Recovery:

No action required.

RxFabrDpResponseMsgQueueAvg

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The average DP Response 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:

This alarm may occur due to persistent overload conditions with respect to database response processing.

Contact the *Customer Care Center* for assistance.

RxFabrDpResponseMsgQueuePeak

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The peak DSR Application's DP Response Message Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum DP Response Message Queue utilization sample taken during the collection interval.

Measurement Scope: Server Group

Recovery:

This alarm may occur due to persistent overload conditions with respect to database response processing.

Contact the *Customer Care Center* for assistance.

RxFabrMsgs

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages received by FABR application.

Collection Interval: 5 min

Peg Condition: For each message successfully de-queued from the application’s internal “Message Event” queue.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolAll

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successfully Resolved to a Destination.

Collection Interval: 5 min

Peg Condition: For each message successfully resolved to a Destination.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolAllMp

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Addresses Successfully Resolved to a Destination by the MP.

Collection Interval: 5 min

Peg Condition: For each message successfully resolved to a Destination by the MP.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolImpi

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IMPI.

Collection Interval: 5 min

Peg Condition: For each message successfully resolved to a Destination using a Routing Entity Type of IMPI.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolImpu

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IMPU.

Collection Interval: 5 min

Peg Condition: For each message successfully resolved to a Destination using a Routing Entity Type of IMPU.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolImsi

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type IMSI.

Collection Interval: 5 min

Peg Condition: For each message successfully resolved to a Destination using a Routing Entity Type of IMSI.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolMsisdn

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Addresses Successful Resolved with Routing Entity type MSISDN.

Collection Interval: 5 min

Peg Condition: For each message successfully resolved to a Destination using a Routing Entity Type of MSISDN.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxFabrResolRateAvg

Measurement Group: Full Address Resolution Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average Addresses Successfully Resolved per second.

Collection Interval: 5 min

Peg Condition: The "average per second" is periodically calculated based on the total number of addresses successfully resolved.

Measurement Scope: Server Group

Recovery:

No action required.

RxFabrResolRatePeak

Measurement Group: Full Address Resolution Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Peak Addresses Successfully Resolved per second.

Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with average successfully resolved message rate, as defined by measurement *RxFabrResolRateAvg*, if the value exceeds the current value for this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: Server Group

Recovery:

No action required.

RxFabrSrvNotiDpCongest

Measurement Group: Full Address Resolution Exception

Measurement Type: Simple

Description: Number of Service Notifications received from ComAgent indicating DP is congested with CL=2 or CL=3.

Collection Interval: 5 min

Peg Condition: When FABR receives Service Notification from ComAgent indicating a DP congestion at CL=2 or CL=3.

Measurement Scope: MP

Recovery:

No action necessary.

TxFabrAbandonRequest

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message that are abandoned.

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception "Abandon Request" is invoked.

Measurement Scope: Server Group

Recovery:

No action necessary.

TxFabrBundledQueryEvents

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Bundled Query Events sent to ComAgent.

Collection Interval: 5 min

Peg Condition: When FABR successfully sends a Bundled query event to ComAgent for processing

Measurement Scope: Server Group

Recovery:

No action required.

TxFabrFwdDefaultDest

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message forwarding attempts using a Default Destination.

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception "Forward route the message with a user-configurable Default Destination" is invoked.

Measurement Scope: Server Group

Recovery:

No action necessary.

TxFabrFwdNochange

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message forwarding attempts without changing the message.

Collection Interval: 5 min

Peg Condition: Each time the Routing Exception "Forward route the message unchanged" is invoked.

Measurement Scope: Server Group

Recovery:

No action necessary.

TxFabrFwdSuccess

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request messages successfully forwarded (all reasons).

Collection Interval: 5 min

Peg Condition: Each time the application successfully enqueues a Request message on the DSR Relay Agent's Request Message Queue.

Measurement Scope: Server Group

Recovery:

If this value is less than *TxFabrMsgAttempt*, then an internal resource error is occurring.

Contact the *Customer Care Center* for assistance.

TxFabrMsgAttempt

Measurement Group: Full Address Resolution Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Diameter Application ID)

Description: Number of Request message forwarding attempts (all reasons).

Collection Interval: 5 min

Peg Condition: Each time the application attempts to enqueue a Request message on the DSR Relay Agent's "Request Message Queue".

Measurement Scope: Server Group

Recovery:

No action necessary.

GLA Exception

The GLA Exception measurement group contains measurements that provide performance information that is specific to the GLA application.

Table 52: GLA Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxGlaDecodeFailures	Number of GLA Requests that could not be processed due to incorrect data in the Diameter message	5 min
RxGlaDatabaseFailures	Number of GLA Requests that could not be processed due to pSBR-B query failure	5 min
RxGlaDatabaseTimeouts	Number of GLA Requests that could not be processed due to pSBR-B query timeout	5 min

RxGlaDecodeFailures

Measurement Group: GLA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of GGRs unsuccessfully processed due to unsupported Application ID, Command Code, Subscriber Info, or other decoding issue.

Collection Interval: 5 min

Peg Condition: During GGR failure handling

Measurement Scope: Server Group

Recovery:

1. While parsing the message, one of the following conditions occurred:
   - The message content was inconsistent with the "Message Length" in the message header.
   - The IMSI contained in the User-Name AVP was considered invalid due to length.

- The MSISDN contained in the MSISDN AVP was considered invalid due to length.

2. These protocol errors can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node. Collect a trace containing the GGR, and determine which node is causing the invalid data.
3. If the problem persists, contact the *Customer Care Center*.

RxGlaDatabaseFailures

Measurement Group: GLA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of GGRs unsuccessfully processed due to queries to pSBR-B receiving a negative acknowledgment.

Collection Interval: 5 min

Peg Condition: During pSBR-B query failures

Measurement Scope: Server Group

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. The status of the Reporting Server's BindingRd should be examined to verify that all SubResources are Available. This will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, contact the *Customer Care Center*.

RxGlaDatabaseTimeouts

Measurement Group: GLA Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of GGRs unsuccessfully processed due to queries to pSBR-B timing out before a response is received.

Collection Interval: 5 min

Peg Condition: During pSBR-B query failures

Measurement Scope: Server Group

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. The status of the Reporting Server's BindingRd should be examined to verify that all SubResources are Available. This will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, contact the *Customer Care Center*.

GLA Performance

The GLA Performance measurement group contains measurements that provide performance information that is specific to the GLA application.

Table 53: GLA Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
TxGlaSuccessMsgs	Number of GLA requests that were successfully processed	5 min
RxGlaResponseMsgQueuePeak	Peak utilization of pSBR-B response queue	5 min
RxGlaResponseMsgQueueAvg	Average Utilization of pSBR-B response queue	5 min
TxGlaSuccessMsgRatePeak	Peak rate of GLA Requests that are successfully processed	5 min
TxGlaSuccessMsgRateAvg	Average rate of GLA Requests that are successfully processed	5 min
RxGlaFailureMsgs	Number of GLA requests that were not successfully process (for any reason)	5 min

TxGlaSuccessMsgs

Measurement Group: GLA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of GGRs successfully processed

Collection Interval: 5 min

Peg Condition: When a GGA is transmitted following a successful query of the pSBR database

Measurement Scope: Server Group

Recovery:

This number can be compared against *RxGlaRequestProcessed* to get a ratio of total input Requests to successfully processed Requests.

RxGlaResponseMsgQueuePeak

Measurement Group: GLA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Peak utilization of GLA's response queue that handles pSBR-B replies.

Collection Interval: 5 min

Peg Condition: Reception of a response Stack Event from pSBR-B.

Measurement Scope: Server Group

Recovery:

1. This number provides an indication of short-term work-rate of the response task. If this value crosses 75%, it indicates that processing rates are increasing and additional capacity may need to be added to the DSR.
2. If the problem persists, contact the *Customer Care Center*.

RxGlaResponseMsgQueueAvg

Measurement Group: GLA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Average utilization of GLA's response queue that handles pSBR-B replies.

Collection Interval: 5 min

Peg Condition: Reception of a response Stack Event from pSBR-B.

Measurement Scope: Server Group

Recovery:

1. This number provides an indication of sustained work-rate of the response task. If this value crosses 50%, it indicates that processing rates are increasing and additional capacity may need to be added to the DSR.
2. If the problem persists, contact the *Customer Care Center*.

TxGlaSuccessMsgRatePeak

Measurement Group: GLA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Peak rate of GGRs successfully processed

Collection Interval: 5 min

Peg Condition: When a GGA is transmitted following a successful query of the pSBR database

Measurement Scope: Server Group

Recovery:

1. This number provides an indication of peak success work-rate of GLA. If can be used to determine when GLA is processing more than a customer's work-rate.

2. If the problem persists, contact the *Customer Care Center*.

TxGlaSuccessMsgRateAvg

Measurement Group: GLA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Average rate of GGRs successfully processed

Collection Interval: 5 min

Peg Condition: When a GGA is transmitted following a successful query of the pSBR database

Measurement Scope: Server Group

Recovery:

1. This number provides an indication of sustained success work-rate of GLA. If can be used to determine when GLA is processing more than a customer's work-rate.
2. If the problem persists, contact the *Customer Care Center*.

RxGlaFailureMsgs

Measurement Group: GLA Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of GGRs unsuccessfully processed due to any problem.

Collection Interval: 5 min

Peg Condition: Any failure during processing

Measurement Scope: Server Group

Recovery:

1. When non-zero, examine other failure measurements (*RxGlaDecodeFailures*, *RxGlaDatabaseFailures*, *RxGlaDatabaseTimeouts*) to isolate reasons for failures
2. Search the Event History for additional information to identify the specific failure.
3. If the problem persists, contact the *Customer Care Center*.

IDIH measurements

The IDIH measurment report contains measurements that provide performance information that is specific to the IDIH feature.

Measurement Tag	Description	Collection Interval
EvIdihNumTtrsSent	Number of TTRs sent to DIH	5 min
EvIdihNumTtrsDeliveryFailed	Number of TTRs that could not be sent to DIH due to ComAgent connection failure	5 min
TmIdihTraceLimitingTime	Amount of time that trace limiting is in force	5 min
TmIdihTraceThrottlingTime	Amount of time that trace throttling is in force	5 min
EvIdihThrottlingTtrsDiscarded	Number of TTRs discarded due to trace throttling	5 min

EvIdihNumTtrsSent

Measurement Group: IDIH

Measurement Type: Simple

Description: The number of TTRs that were sent from DSR to DIH.

Collection Interval: 5 min

Peg Condition: Each time a TTR is successfully transmitted from DSR to DIH.

Recovery:

No action required

EvIdihNumTtrsDeliveryFailed

Measurement Group: IDIH

Measurement Type: Simple

Description: The number of TTRs that could not be sent from DSR to DIH due to the failure of the ComAgent link.

Collection Interval: 5 min

Peg Condition: Each time a TTR cannot be successfully transmitted from DSR to DIH.

Recovery:

Re-establish the ComAgent link to DIH.

TmIdihTraceLimitingTime

Measurement Group: IDIH

Measurement Type: Duration

Description: The amount of time that trace limiting is active.

Collection Interval: 5 min

Peg Condition: Each time trace limiting is activated and stopped when trace limiting is de-activated.

Recovery:

No action required

TmIdihTraceThrottlingTime

Measurement Group: IDIH

Measurement Type: Duration

Description: The amount of time that trace throttling is active.

Collection Interval: 5 min

Peg Condition: Each time trace throttling is activated and stopped when trace throttling is de-activated.

Recovery:

No action required

EvIdihThrottlingTtrsDiscarded

Measurement Group: IDIH

Measurement Type: Simple

Description: The number of TTRs discarded due to trace throttling.

Collection Interval: 5 min

Peg Condition: Each time a TTR is discarded due to trace throttling.

Recovery:

No action required

IP Front End (IPFE) Exception measurements

The "IPFE Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events specific to the IPFE application. Measurements such as the following are included in this group.

Table 54: IPFE Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
PcapDroppedPackets	Number of ARP/ICMP/ICMPv6 control packets dropped	5 min
ThrottledPackets	Number of packets dropped due to throttling	5 min, 30 min, 60 min
TsaUnexpctedSctp	Number of SCTP packets sent to a TSA configured as “TCP Only”.	5 min

Measurement Tag	Description	Collection Interval
TsaUnexpctedTcp	Number of TCP packets sent to a TSA configured as “SCTP Only”.	5 min
TxReject	Number of new associations rejected	5 min
TxRejectSctp	Number of new SCTP associations rejected	5 min

PcapDroppedPackets

Measurement Group: IPFE Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: ARP/ICMP/ICMPv6 control packets dropped. The pcap library listens for packets on the network interfaces on behalf of the IPFE. If the network interface receives more packets than it can handle, the library will drop packets and increase a dropped packet counter.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time the IPFE drops an ARP/ICMP/ICMPv6 control packet.

Measurement Scope: Network, NE, Server Group

Recovery:

1. In the unlikely event that counts should appear for this measurement, network diagnostics should be performed.
2. For further assistance, contact the *Customer Care Center*.

ThrottledPackets

Measurement Group: IPFE Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of packets dropped due to throttling

Collection Interval: 5 min, 30 min, 60 min

Peg Condition: When a packet is dropped to limit excessive IPFE CPU

Measurement Scope: Network

Recovery:

Increase DSR Capacity.

TsaUnexpctedSctp

Measurement Group: IPFE Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: Number of SCTP packets sent to a TSA configured as “TCP Only”.

Collection Interval: 5 minutes

Peg Condition: Incremented when an SCTP packet is received for a TSA configured as “TCP Only”.

Measurement Scope: Network, NE, Server Group

Recovery:

Check client configuration for clients attempting SCTP associations with a TCP-only TSA.

TsaUnexpctedTcp

Measurement Group: IPFE Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: Number of TCP packets sent to a TSA configured as “SCTP Only”.

Collection Interval: 5 minutes

Peg Condition: Incremented when a TCP packet is received for a TSA configured as “SCTP Only”.

Measurement Scope: Network, NE, Server Group

Recovery:

Check client configuration for clients attempting TCP connections on an SCTP-only TSA.

TxReject

Measurement Group: IPFE Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: Number of new associations rejected. The IPFE rejects new associations when there are no available applications servers for the target set address. The associated alarm, *5009 - No available servers in target set*, will also be issued.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time the IPFE rejects a new association for a target set address.

Measurement Scope: Network, NE, Server Group

Recovery:

Check the status of the application servers by navigating to the **Status & Manage > Server** page.

TxRejectSctp

Measurement Group: IPFE Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: New SCTP associations rejected.

Collection Interval: 5 minutes

Peg Condition: Incremented when an SCTP association is rejected.

Measurement Scope: Network, NE, Server Group

Recovery: None required

IP Front End (IPFE) Performance measurements

The "IPFE Performance" measurement group contains measurements that provide performance information that is specific to the IPFE application. Counts for various expected/normal messages and events are included in this group. Measurements such as the following are included.

Table 55: IPFE Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
AsNewAssociations	Number of new associations for each server	5 min
AsNewAssociationsSctp	Number of new SCTP associations for each server	5 min
IpfeNewAssociations	Number of new associations for the IPFE	5 min
IpfeNewAssociationsSctp	Number of new SCTP associations for the IPFE	5 min
RxIpfeBytes	Number of bytes received by the IPFE	5 min
RxIpfeBytesSctp	Number of SCTP bytes received by the IPFE	5 min
RxIpfePackets	Number of packets received by the IPFE	5 min
RxTsaBytes	Number of bytes received for each TSA	5 min

Measurement Tag	Description	Collection Interval
RxTsaBytesSctp	Number of SCTP bytes received for each TSA	5 min
RxTsaPackets	Number of packets received for each TSA	5 min
RxTsaPacketsSctp	Number of SCTP packets received for each TSA	5 min
TsaNewAssociations	Number of new associations for each TSA	5 min
TsaNewAssociationsSctp	Number of new SCTP associations for each TSA	5 min
TxAsBytes	Number of bytes sent for each server	5 min
TxAsBytesSctp	Number of SCTP bytes sent for each server	5 min
TxAsPackets	Number of packets sent for each server	5 min
TxAsPacketsSctp	Number of SCTP packets sent for each server	5 min

AsNewAssociations

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Application Server ID)

Description: New associations for each server

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time the IPFE associates a client packet with an application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

AsNewAssociationsSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Application Server ID)

Description: New SCTP associations for each server,

Collection Interval: 5 minutes

Peg Condition: Incremented when a new SCTP association is established for an application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

IpfeNewAssociations

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: New associations for the IPFE

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time the IPFE associates a client packet with an application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

IpfeNewAssociationsSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: New SCTP associations for the IPFE ,

Collection Interval: 5 minutes

Peg Condition: Incremented when a new SCTP association is established through an IPFE.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxIpfeBytes

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of bytes received by the IPFE.

Collection Interval: 5 minutes, 30 minutes, 60 minutes

Peg Condition: The measurement is incremented by one for each byte the IPFE receives.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxIpfeBytesSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of SCTP bytes received by the IPFE.

Collection Interval: 5 minutes, 30 minutes, 60 minutes

Peg Condition: Incremented by the packet payload size when an SCTP packet is received by the IPFE.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxIpfePackets

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Packets received by the IPFE

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one for each packet the IPFE receives.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxTsaBytes

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: Bytes received for each TSA.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time a byte is received for a particular target set address.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxTsaBytesSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: SCTP bytes received for each TSA.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time an SCTP byte is received for a particular target set address.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxTsaPackets

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: Packets received for each TSA

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time a packet is received for a particular TSA.

Measurement Scope: Network, NE, Server Group

Recovery: None required

RxTsaPacketsSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: SCTP packets received for each TSA.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time an SCTP packet is received for a particular TSA.

Measurement Scope: Network, NE, Server Group

Recovery: None required

TsaNewAssociations

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: New associations for each target set address

Collection Interval:

Peg Condition: This measurement is incremented by one each time the IPFE associates a client packet with a target set address.

Measurement Scope: Network, NE, Server Group

Recovery: None required

TsaNewAssociationsSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: New SCTP associations for each TSA.

Collection Interval: 5 minutes

Peg Condition: Incremented when a new SCTP association is established for a TSA.

Measurement Scope: Network, NE, Server Group

Recovery: None required

TxAsBytes

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Bytes sent for each server

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time a byte is sent to a particular application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

TxAsBytesSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by TSA ID)

Description: SCTP bytes sent for each server

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time an SCTP byte is sent to a particular application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

TxAsPackets

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Application Server ID)

Description: Packets sent for each server.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time a packet is sent to a particular application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

TxAsPacketsSctp

Measurement Group: IPFE Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Application Server ID)

Description: SCTP packets sent for each server.

Collection Interval: 5 minutes

Peg Condition: This measurement is incremented by one each time an SCTP packet is sent to a particular application server.

Measurement Scope: Network, NE, Server Group

Recovery: None required

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

Table 56: Message Copy Measurement Report Fields

Measurement Tag	Description	Collection Interval
DASCopyAnswerRx	Total number of DAS Copy Answers received.	5 min
DASCopyDiscarded	Total number of Message Copy failures because of any error (no Answer received, the result code in the Answer didn't match provisioning).	5 min
DASCopyFailureMCCSNotProvisioned	Total amount of DAS Copy failures due to the copied message not finding a provisioned MCCS.	5 min
DASCopyFailureMPCong	Total number of DAS Copy Failures because the MP was congested.	5 min
DASCopyFailurePeerApplIdUnsup	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.	5 min
DASCopyFailureRLNotProv	Total number of DAS Copy Failures because the route list is not provisioned.	5 min
DASCopyFailureSizeExceeded	Total amount of DAS Copy failures due to the copied message size configured for the system.	5 min
DASCopyRetransmits	Total number of DAS Copy retransmits.	5 min

Measurement Tag	Description	Collection Interval
DASCopyRetransmitsExceeded	Total number of times the DAS Copy retransmits exceeded the configured max number of retransmits.	5 min
DASCopyTx	Total number of DAS Copies forwarded.	5 min
DASCopyValidAnswer	Total number of DAS Copy transactions completed (a Copy Pending Transaction has been paired with a qualified Answer from the DAS peer).	5 min
TxMsgCopyQueueAve	Average Message Copy Queue utilization (0-100%) measured during the collection interval.	5 min
TxMsgCopyQueueFullDiscard	Total number of DAS Request messages discarded because the Message Copy queue was full.	5 min
TxMsgCopyQueuePeak	Peak Message Copy Queue utilization (0-100%) measured during the collection interval.	5 min

DASCopyAnswerRx

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:

No action required.

This measurement is an indication of the Message Copy response traffic load being processed by the MP.

DASCopyDiscarded

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. Contact the *Customer Care Center* for assistance.

DASCopyFailureMCCSNotProvisioned

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, contact the *Customer Care Center*.

DASCopyFailureMPCong

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. Contact the *Customer Care Center* for assistance.

DASCopyFailurePeerApplIdUnsup

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. Contact the *Customer Care Center* for assistance.

DASCopyFailureSizeExceeded

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. Contact the *Customer Care Center* for assistance.

DASCopyFailureRLNotProv

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. Contact the *Customer Care Center* for assistance.

DASCopyRetransmits

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. Contact the *Customer Care Center* for assistance.

DASCopyRetransmitsExceeded

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. Contact the *Customer Care Center* for assistance.

DASCopyTx

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:

No action required.

This measurement is an indication of the Message Copy traffic load being processed by the MP.

DASCopyValidAnswer

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. Contact the *Customer Care Center* for assistance.

TxMsgCopyQueueAve

Measurement Group: DAS

Measurement Type: Average

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:

No action required.

This is an diagnostic indicator of the amount of traffic load being processed by the Message Copy feature.

TxMsgCopyQueueFullDiscard

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:

No action required.

This is an diagnostic indicator of the amount of traffic load being processed by the Message Copy feature.

TxMsgCopyQueuePeak

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:

No action required.

This is an 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.

Table 57: Message Priority Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvConnPeerUnsuppMp	The number of times an ingress Request was received on a connection configured to read message priority from the ingress message, and the peer did not support the UCMP feature. **Note:** In this case, DSR assigns the default priority of 0 to all such requests.	5 min
EvConnUnexpMp	The number of times an ingress Request message was received with a priority of “3”, when the peer supports UCMP feature.	5 min
RxMsgPri0ApplRule	Number of Request messages set to priority "0" as a result of ART processing	5 min
RxMsgPri0Ingress	Total number of ingress messages assigned message priority 0.	5 min
RxMsgPri0PeerRule	Number of Request messages set to priority “0” as a result of PRT processing.	5 min
RxMsgPri1ApplRule	Number of Request messages set to priority "1" as a result of ART processing	5 min
RxMsgPri1Ingress	Total number of ingress messages assigned message priority 1.	5 min
RxMsgPri1PeerRule	Number of Request messages set to priority “1” as a result of PRT processing.	5 min
RxMsgPri2ApplRule	Number of Request messages set to priority "2" as a result of ART processing	5 min
RxMsgPri2Ingress	Total number of ingress messages assigned message priority 2.	5 min
RxMsgPri2PeerRule	Number of Request messages set to priority “2” as a result of PRT processing.	5 min

ExConnPeerUnsuppMp

Measurement Group: Message Priority

Measurement Type: Simple

Description: The number of times an ingress Request was received on a connection configured to read message priority from the ingress message, and the peer did not support the UCMP feature.

Note: In this case, DSR assigns the default priority of 0 to all such requests.

Collection Interval: 5 min

Peg Condition: Pegged when a connection is configured to read message priority from ingress message and the peer does not support UCMP feature.

Measurement Scope: Server Group

Recovery:

1. Verify that the peer is a DSR
   - Product-Name is reported as "Eagle XG DSR", in the Event Additional Information.
   - Vendor-Id is reported as 323 (Tekelec).
2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.
   - Call *Customer Care Center* and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   - If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call *Customer Care Center*.
   - If the reported Firmware-Version is less than the minimum required DSR software version, call *Customer Care Center* to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to "None".

ExConnUnexpMp

Measurement Group: Message Priority

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times an ingress Request message was received with a priority of "3", when the peer supports UCMP feature.

Collection Interval: 5 min

Peg Condition: Pegged when a peer supports UCMP feature and an ingress Request message was received with a priority of "3".

Measurement Scope: Server Group

Recovery:

1. Verify that the peer is a DSR

- Product-Name is reported as “Eagle XG DSR”, in the Event Additional Information.
- Vendor-Id is reported as 323 (Tekelec).

2. Verify that the Firmware-Revision reported in the Event Additional Information represents a DSR software version that supports the Message Priority Feature.
   - Call *Customer Care Center* and obtain the minimum DSR software version that supports Message Priority and compare with this information.
   - If the reported Firmware-Version is greater than or equal to the minimum required DSR software version, call *Customer Care Center*.
   - If the reported Firmware-Version is less than the minimum required DSR software version, call *Customer Care Center* to seek advice on whether the peer DSR needs to be upgraded, or whether the Message Priority Setting for this Transport Connection or Peer Node needs to be changed to “None”.

RxMsgPri0ApplRule

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:

No action required.

RxMpMsgPri0

Measurement Group: Message Priority

Measurement Type: Simple

Measurement Dimension: Single

Description: Total number of ingress messages assigned message priority 0.

Collection Interval: 5 min

Peg Condition: Pegged when an ingress message is assigned a priority of 0.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxMsgPri0PeerRule

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:

No action necessary.

RxMsgPri1ApplRule

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:

No action required.

RxMpMsgPri1

Measurement Group: Message Priority

Measurement Type: Simple

Measurement Dimension: Single

Description: Total number of ingress messages assigned message priority 1.

Collection Interval: 5 min

Peg Condition: Pegged when an ingress message is assigned a priority of 1.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxMsgPri1PeerRule

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:

No action necessary.

RxMsgPri2ApplRule

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:

No action required.

RxMpMsgPri2

Measurement Group: Message Priority

Measurement Type: Simple

Measurement Dimension: Single

Description: Total number of ingress messages assigned message priority 2.

Collection Interval: 5 min

Peg Condition: Pegged when an ingress message is assigned a priority of 2.

Measurement Scope: Server Group

Recovery:

No action necessary.

RxMsgPri2PeerRule

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:

No action necessary.

Message Processor (MP) Performance measurements

The MP Performance measurement report contains measurements that provide performance information for an MP server.

Table 58: MP Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
EvDiameterProcessAvg	The average Diameter process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.	5 min
EvDiameterProcessPeak	The peak Diameter process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.	5 min
EvLongTimeoutPtrPoolAvg	The average Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.	5 min

Measurement Tag	Description	Collection Interval
EvLongTimeoutPtrPoolPeak	The peak Diameter Long Timeout PTR Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
EvMpCongestionEntered	Number of times that the MP became congested (regardless of severity level).	5 min
EvMpCongestionLevel1Entered	The number of times that the local DA-MP entered CPU congestion level 1.	5 min
EvMpCongestionLevel2Entered	The number of times that the local DA-MP entered CPU congestion level 2.	5 min
EvMpCongestionLevel3Entered	The number of times that the local DA-MP entered CPU congestion level 3.	5 min
EvMpDangerOfCongestionEntered	The number of times that the local DA-MP entered danger of CPU congestion.	5 min
EvPduPoolAvg	The average Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
EvPduPoolPeak	The peak Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
EvPtrPoolAvg	The average Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
EvPtrPoolPeak	The peak Diameter PTR Buffer Pool utilization (0-100%) measured during the collection interval.	5 min
EvStasisModeMaxConnections	The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to the maximum number of connections on the DA-MP.	5 min
EvStasisModeMpCongestion	The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to MP Congestion.	5 min

Measurement Tag	Description	Collection Interval
RxAnswerMsgQueueAvg	The average Answer Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxAnswerMsgQueuePeak	The peak Answer Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxMsgRateAvgMp	The average MP ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero application ID).	5 min
RxMsgRatePeakMp	The peak Ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero application ID).	5 min
RxRequestMsgQueueAvg	The average Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
RxRequestMsgQueuePeak	The peak Request Message Queue utilization (0-100%) measured during the collection interval.	5 min
TmAnswerTimeAvg	Average time (in microseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.	5 min
TmAnswerTimePeak	Peak time (in microseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.	5 min
TmMpCongestion	Total time (in milliseconds) spent in local MP congestion state.	5 min
TmMpCongestionLevel1	The total time (in seconds) the local DA-MP was in CPU congestion level	5 min

Measurement Tag	Description	Collection Interval
	1. This value will appear as an aggregate value retrieved from all DA-MPs in a Network Element.	
TmMpCongestionLevel2	The total time (in seconds) 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.	5 min
TmMpCongestionLevel3	The total time (in seconds) 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.	5 min
TmMpDangerOfCongestion	The total time (in milliseconds) the local DA-MP was in danger of CPU congestion. This will appear as an aggregate value retrieved from all DA-MPs for OAM Network Element.	5 min
TmRequestTimeAvg	Average time (in microseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.	5 min
TmRequestTimePeak	Peak time (in microseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.	5 min
TxAllConnQueueAvg	The average All-Connections Event Queue utilization (0-100%) measured during the collection interval.	5 min
TxAllConnQueuePeak	The peak All-Connections Event Queue utilization (0-100%) measured during the collection interval.	5 min
TxRerouteQueueAvg	The average Reroute Queue utilization (0-100%) measured during the collection interval.	5 min
TxRerouteQueuePeak	The peak Reroute Queue utilization (0-100%) measured during the collection interval.	5 min

EvDiameterProcessAvg

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average Diameter Process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.

Collection Interval: 5 min

Peg Condition: The average of all Diameter process CPU 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. Contact the *Customer Care Center* for assistance if needed.

EvDiameterProcessPeak

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak Diameter process CPU utilization (0-100%) measured during the collection interval. The Diameter process is responsible for all Diameter-related processing.

Collection Interval: 5 min

Peg Condition: The maximum Diameter process CPU 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. Contact the *Customer Care Center* for assistance if needed.

EvLongTimeoutPtrPoolAvg

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, contact the *Customer Care Center*.

EvLongTimeoutPtrPoolPeak

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, contact the *Customer Care Center*.

EvMpCongestionEntered

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times that the MP became congested (regardless of severity level).

Collection Interval: 5 min

Peg Condition: Each time Alarm *22200 - Local MP Congestion* transitions from cleared to asserted with severity CL1.

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. The Diameter process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

EvMpCongestionLevel1Entered

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* transitions from "cleared" or asserted with severity "Info" to asserted with severity "Minor".

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, contact the *Customer Care Center*.

EvMpCongestionLevel2Entered

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* transitions from "cleared" or asserted with severity "Info" or "Minor" to asserted with severity "Major".

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, contact the *Customer Care Center*.

EvMpCongestionLevel3Entered

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* transitions from "cleared" or asserted with severity "Info", "Minor", or "Major" to asserted with severity "Critical".

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, contact the *Customer Care Center*.

EvMpDangerOfCongestionEntered

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of times that the local DA-MP entered danger of CPU congestion.

Collection Interval: 5 min

Peg Condition: Each time Alarm *22200 - Local MP Congestion* transitions from "cleared" to asserted with severity “Info”.

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

EvPduPoolAvg

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all Diameter PDU 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. Contact the *Customer Care Center* for assistance if needed.

EvPduPoolPeak

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak Diameter PDU Buffer Pool utilization (0-100%) measured during the collection interval.

A PDU is allocated to each message that arrives at an MP and is de-allocated when message processing completes. This measurement is useful for evaluating whether persistent network problems exist. In general, PDU buffers are engineered to match the processing capacity of the MP. If network problems exist, delaying the off-loading of egress messages from the MP, then PDUs/messages will sit in internal Diameter queues.

Collection Interval: 5 min

Peg Condition: The maximum Diameter PDU 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. Contact the *Customer Care Center* for assistance if needed.

EvPtrListAvg

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. Contact the *Customer Care Center* for assistance if needed.

EvPtrListPeak

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. Contact the *Customer Care Center* for assistance if needed.

EvStasisModeMaxConnExceeded

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The maximum number of active Diameter connections supported by a DA-MP has been exceeded. The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to the maximum number of connections on the DA-MP.

Collection Interval: 5 min

Peg Condition: This measurement is incremented when the A DA-MP is sending IPFE a "heartbeat" message and it has determined that the number of Diameter connections established has reached the maximum number supported by the DA-MP since the last "heartbeat" message was sent. A DA-MP will send a "heartbeat" message indicating a STASIS availability status when it has reached its maximum number of active Diameter connections.

Measurement Scope: Server Group

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 the *Customer Care Center*.

EvStasisModeMpCongestion

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The DA-MP is in MP Congestion due to high traffic rates. The number of times DA-MP requested IPFE to cease distributing Diameter connections to the DA-MP due to MP Congestion.

Collection Interval: 5 min

Peg Condition: This measurement is incremented when the A DA-MP is sending IPFE a "heartbeat" message and it has been determined that its Congestion Level has transitions from CL0 (No Congestion) since the last heartbeat message sent. A DA-MP will send a "heartbeat" message indicating STASIS availability status when it's Congestion Level is greater than CL0.

Measurement Scope: Server Group

Recovery:

1. The traffic rate needs to be decreased.
2. Contact the *Customer Care Center* for assistance.

RxAnswerMsgQueueAvg

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. Contact the *Customer Care Center* for assistance if needed.

RxAnswerMsgQueuePeak

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. Contact the *Customer Care Center* for assistance if needed.

RxMsgRateAvgMp

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average MP ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).

Collection Interval: 5 min

Peg Condition: The average of all MP ingress message rate 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. Contact the *Customer Care Center* for assistance if needed.

RxMsgRatePeakMp

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak ingress message rate (in messages per second) measured during the collection interval. The ingress message rate is the number of ingress Diameter messages that are targeted for Relay Agent routing (non-zero Application ID).

Collection Interval: 5 min

Peg Condition: The maximum ingress message rate (messages per second) 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. Contact the *Customer Care Center* for assistance if needed.

RxRequestMsgQueueAvg

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. Contact the *Customer Care Center* for assistance if needed.

RxRequestMsgQueuePeak

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. Contact the *Customer Care Center* for assistance if needed.

TmAnswerTimeAvg

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average time (in milliseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.

Note: This is the average cross-MP delay for answers during the measurement period excluding ethernet/IP stack ingress and egress processing time.

Collection Interval: 5 min

Peg Condition: Timing started when an ingress Answer message is read from the connection socket. Timing stopped when the matching egress Answer message is written to the connection socket. The difference between the two times is used to update the average.

Measurement Scope: Server Group

Recovery:

1. If this measurement indicates an excessive average cross-MP delay, examine the DIAM KPIs to determine if the system is under excessive load.
2. Examine the Peer Routing Rules to determine if there are an excessive number of rules.
3. Contact the *Customer Care Center* for assistance if needed.

TmAnswerTimePeak

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Peak time (in milliseconds) to process an Answer message. This is the time from when a Diameter Answer message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.

Note: This is the peak cross-MP delay for answers during the measurement period excluding ethernet/IP stack ingress and egress processing time.

Collection Interval: 5 min

Peg Condition: Timing started when an ingress Answer message is read from the connection socket. Timing stopped when the matching egress Answer message is written to the connection socket. This measurement is pegged if the difference is larger than the current value of the measurement.

Measurement Scope: Server Group

Recovery:

No action required.

TmMpCongestion

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Total time (in millisecondsseconds) spent in local MP congestion state.

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 *22200 - Local MP Congestion* is asserted (regardless of severity level).
2. Alarm *22200 - Local MP Congestion* is asserted with severity Minor (local MP congestion level CL0 to CL1 transition).

The time duration interval stops when one of the following conditions occurs:

1. The collection interval for the measurement ends and alarm *22200 - Local MP Congestion* is asserted (regardless of severity level).
2. Alarm *22200 - Local MP Congestion* is cleared (local MP congestion level CL1 to CL0 transition).

When a time duration interval completes, the time measured is added to the total measurement value.

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. The Diameter Process may be experiencing problems. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, contact the *Customer Care Center*.

TmMpCongestionLevel1

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total time (in seconds) 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 *22200 - Local MP Congestion* is already asserted with severity "Minor".
- Alarm *22200 - Local MP Congestion* 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* is already asserted with severity "Minor".
- Alarm *22200 - Local MP Congestion* 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.

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, contact the *Customer Care Center*.

TmMpCongestionLevel2

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total time (in seconds) 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* is already asserted with severity "Major".
- Alarm *22200 - Local MP Congestion* 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* is already asserted with severity "Major".
- Alarm *22200 - Local MP Congestion* 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.

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, contact the *Customer Care Center*.

TmMpCongestionLevel3

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total time (in seconds) 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* is already asserted with severity "Critical".
- Alarm *22200 - Local MP Congestion* 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* is already asserted with severity "Critical".
- Alarm *22200 - Local MP Congestion* 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.

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, contact the *Customer Care Center*.

TmMpDangerOfCongestion

Measurement Group: MP Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The total time (in milliseconds) the local DA-MP was in danger of CPU congestion. This will appear as an aggregate value retrieved from all DA-MPs for OAM Network Element.

Collection Interval: 5 min

Peg Condition:

The "time interval" starts when one of the following conditions occurs:

- A new "collection interval" for the measurement begins and Alarm *22200 - Local MP Congestion* is already asserted with severity "Info".
- Alarm *22200 - Local MP Congestion* is asserted with severity "Info" (onset of local DA-MP danger of CPU congestion).

The "time interval" stops when one of the following conditions occurs:

- The "collection interval" for the measurement ends and Alarm *22200 - Local MP Congestion* is already asserted with severity "Info".
- Alarm *22200 - Local MP Congestion* is cleared (abatement of local DA-MP danger of CPU congestion).

When the "time interval" completes, the time measured is added to the measurement value.

Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the DA-MP server status from **Main Menu** > **Status & Manage** > **Server Status**.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. Each DA-MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. Monitor the ingress traffic rate of each DA-MP from **Main Menu** > **Status & Manage** > **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log from **Main Menu** > **Alarms & Events**.
5. If the problem persists, contact the *Customer Care Center*.

TmRequestTimeAvg

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average time (in milliseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.

Note: This is the average cross-MP delay for Requests during the measurement period excluding ethernet/IP stack ingress and egress processing time.

Collection Interval: 5 min

Peg Condition: Timing started when an ingress message is read from the connection socket. Timing stopped when the matching egress message is written to the connection socket. The difference between the two times is used to update the average.

Measurement Scope: Server Group

Recovery:

1. If this measurement indicates an excessive average cross-MP delay, examine the DIAM KPIs to determine if the system is under excessive load.
2. Examine the Peer Routing Rules to determine if there are an excessive number of rules.
3. Contact the *Customer Care Center* for assistance if needed.

TmRequestTimePeak

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Peak time (in milliseconds) to process a Request message. This is the time from when a Diameter Request message is read from the ingress peer's SCTP/TCP socket until it is sent to the egress peer's SCTP/TCP socket.

Note: This is the peak cross-MP delay for Requests during the measurement period excluding ethernet/IP stack ingress and egress processing time.

Collection Interval: 5 min

Peg Condition: Timing started when an ingress request message is read from the connection socket. Timing stopped when the matching egress request message is written to the connection socket. This measurement is pegged if the difference is larger than the current value of the measurement.

Measurement Scope: Server Group

Recovery:

No action required.

TxAllConnQueueAvg

Measurement Group: MP Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average All-Connections Event Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The average of all All-Connections Event Queue utilization samples taken during the collection interval.

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, contact the *Customer Care Center*.

TxAllConnQueuePeak

Measurement Group: MP Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak All-Connections Event Queue utilization (0-100%) measured during the collection interval.

Collection Interval: 5 min

Peg Condition: The maximum of all All-Connections Event Queue utilization samples taken during the collection interval.

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, contact the *Customer Care Center*.

TxRerouteQueueAvg

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, contact the *Customer Care Center*.

TxRerouteQueuePeak

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, contact the *Customer Care Center*.

OAM Alarm measurements

Table 59: OAM Alarm measurements

Measurement Tag	Description	Collection Interval
Alarm Crit	The number of critical alarms.	5 minutes

Measurement Tag	Description	Collection Interval
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 60: 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	5 minutes

Measurement Tag	Description	Collection Interval
	physical RAM, in which case, swapping will occur.	
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
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

P-DRA Diameter Usage measurements

The P-DRA Diameter Usage measurement report contains measurements that provide performance information that is specific to the P-DRA Diameter protocol.

Table 61: P-DRA Diameter Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
PdraGxTopoHidingApplied	Number of messages received on Gx interface on which topology hiding has been applied by P-DRA.	5 min
PdraGxpTopoHidingApplied	Number of Gx-Prime CC Request messages on which topology hiding is applied.	5 min
PdraRxTopoHidingApplied	Number of messages received on Rx interface on which topology hiding has been applied by P-DRA.	5 min
RxBindCapApn2PcrfPool	Number of times a given APN is successfully mapped to a PCRF Pool	5 min
RxBindCap2PcrfSubPool	Number of binding capable session initiation requests that were mapped to a PCRF Sub-Pool by a given PCRF Sub-Pool Selection Rule	5 min
RxBindCapPcrfPool2Prt	Number of binding capable session initiation requests that are routed using a PRT table chosen as a result of PCRF Pool or PCRF Sub-Pool mapping to the PRT.	5 min
RxCcrInitNoImsiMsgs	Number of CCR Initial messages received without IMSI.	5 min
RxPdra5002FromPcrf	Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a PCRF	5 min
RxPdra5002FromPolicyClient	Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a policy client.	5 min
RxPdraAarMsgs	Number of AAR messages received by PDRA.	5 min
RxPdraAsrMsgs	Number of ASR messages received by PDRA.	5 min
RxPdraCcrInitMsgs	Number of CCR Initial messages received by PDRA.	5 min
RxPdraCcrTerminateMsgs	Number of CCR Termination messages received by PDRA.	5 min
RxPdraCcrUpdateMsgs	Number of CCR Update messages received by PDRA.	5 min

Measurement Tag	Description	Collection Interval
RxPdraGxpBindingSuccess	Number of Gx-Prime CCR Initial messages processed by PDRA against binding key priorities	5 min
RxPdraGxpCcrInitMsgs	Number of Gx-Prime CCR Initial messages processed by PDRA	5 min
RxPdraGxpCcrUpdateMsgs	Number of Gx-Prime CCR Update messages received by PDRA	5 min
RxPdraGxpCcrTerminateMsgs	Number of Gx-Prime CCR Termination messages received by PDRA	5 min
RxPdraMsgRateAvg	Average Diameter ingress message processing rate of P-DRA during the collection interval.	5 min
RxPdraMsgRatePeak	Peak Diameter ingress message processing rate of P-DRA during the collection interval.	5 min
RxPdraRarGxMsgs	Number of RAR messages received by PDRA for Gx interface.	5 min
RxPdraRarRxMsgs	Number of RAR messages received by PDRA for Rx interface.	5 min
RxPdraStrMsgs	Number of STR messages received by PDRA.	5 min
TxPdraGxRarQuery	Number of Gx RAR requests initiated by P-DRA for the purposes of querying for session existence at the policy client.	5 min
TxPdraGxRarRelease	Number of Gx RAR requests initiated by P-DRA for the purposes of releasing a session as a result of an error in the P-DRA.	5 min

PdraGxTopoHidingApplied

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of messages received on Gx interface on which topology hiding has been applied by P-DRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time topology hiding is applied when a message from Gx interface is processed by the application.

Measurement Scope: All

Recovery:

No action necessary.

PdraGxpTopoHidingApplied

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CC Request messages on which topology hiding is applied.

Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime CC request message is processed by the P-DRA application and topology hiding is applied on the message.

Measurement Scope: All

Recovery:

No action required.

PdraRxTopoHidingApplied

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of messages received on Rx interface on which topology hiding has been applied by P-DRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time topology hiding is applied when a message from Rx interface is processed by the application.

Measurement Scope: All

Recovery:

No action necessary.

RxBindCapApn2PcrfPool

Measurement Group: P-DRA Diameter Usage

Description: The number of times a given APN is successfully mapped to PCRF pool.

Measurement Type: Simple

Measurement Dimension: Arrayed (by APN)

Collection Interval: 5 min

Peg Condition: Each time a binding capable session initiation request is successfully mapped to a PCRF Pool (a configured APN), regardless of whether or not the rule matching results in the selection of a PCRF Pool or a PCRF Sub-Pool.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement shows the distribution of binding capable session initiation requests across the range of configured APNs.
2. Contact the *Customer Care Center*.

RxBindCapPcrfPool2Prt

Measurement Group: P-DRA Diameter Usage

Description: The number of binding capable session initiation requests that are routed using a PRT table chosen as a result of PCRF Pool or PCRF Sub-Pool mapping to the PRT.

Measurement Type: Simple

Measurement Dimension: Arrayed (by PCRF Pool or Sub-Pool)

Collection Interval: 5 min

Peg Condition: Each time a binding capable session initiation request is routed using a PRT table selected on the basis of the PCRF Pool or Sub-Pool, regardless of whether or not the request was routed successfully.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement shows the distribution of binding capable session initiation requests that are routed using a given Peer Routing Table at each site.
2. Contact the *Customer Care Center*.

RxBindCap2PcrfSubPool

Measurement Group: P-DRA Diameter Usage

Description: The number of binding capable session initiation requests that were mapped to a PCRF Sub-Pool by a given PCRF Sub-Pool Selection Rule.

Measurement Type: Simple

Measurement Dimension: Arrayed (by PCRF Sub-Pool Selection Rule)

Collection Interval: 5 min

Peg Condition: Each time a binding capable session initiation request is successfully mapped to a PCRF Sub-Pool as a result of a given PCRF Sub-Pool Selection Rule, regardless of whether the request is routed to the Sub-Pool or routed elsewhere due to an existing binding.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement shows the distribution of binding capable session initiation requests for which a new binding would route to a PCRF Sub-Pool across the set of PCRF Sub-Pool Selection Rules.
2. Contact the *Customer Care Center*.

RxCcrInitNoImsiMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of CCR Initial messages without IMSI.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time P-DRA processes a CCR Initial message in which IMSI is not present.

Measurement Scope: All

Recovery:

No action necessary.

RxPdra5002FromPcrf

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a PCRF

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time a PCRF responds to a Diameter request with a 5002 response code.

Measurement Scope: All

Recovery:

No action necessary.

RxPdra5002FromPolicyClient

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of 5002 DIAMETER_UNKNOWN_SESSION_ID responses received from a policy client.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time a policy client responds to a Diameter request with a 5002 response code.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraAarMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of AAR messages received by PDRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives an AAR message.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraAsrMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ASR messages received by PDRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives an ASR message.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraCcrInitMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of CCR Initial messages received by PDRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives a CCR Initial message.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraCcrTerminateMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of CCR Termination messages received by PDRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives a CCR Termination message.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraCcrUpdateMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of CCR Update messages received by PDRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives a CCR Update message.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraGxpBindingSuccess

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CCR Initial messages processed by P-DRA against binding key priorities.

Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime CCR-I message is processed by P-DRA.

Note: The number is sorted and stored in 5 buckets:

- Bucket 1 holds the number of Gx-Prime CCR-I messages that lead to successful binding record findings corresponding to the binding keys with the highest (1) priority.
- Bucket 2 (or 3 or 3) holds the number of Gx-Prime CCR-I messages that lead to successful binding record findings corresponding to the configured binding keys with priority 2 (or 3 or 4).
- Bucket 5 holds the number of Gx-Prime CCR-I messages that lead NO binding record finding after exhausting all binding keys.

Measurement Scope: All

Recovery:

No action required.

RxPdraGxpCcrInitMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CCR Initial messages processed by P-DRA.

Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime CCR-I message is processed by P-DRA.

Measurement Scope: All

Recovery:

No action required.

RxPdraGxpCcrUpdateMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CCR Update messages processed by P-DRA against binding key priorities.

Collection Interval: 5 min

Peg Condition: Each time the P-DRA Application receives a Gx-Prime CCR Update message.

Measurement Scope: All

Recovery:

No action required.

RxPdraGxpCcrTerminateMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CCR Termination messages received by P-DRA against binding key priorities.

Collection Interval: 5 min

Peg Condition: Each time the P-DRA Application receives a Gx-Prime CCR Termination message.

Measurement Scope: All

Recovery:

No action required.

RxPdraMsgRateAvg

Measurement Group: P-DRA Diameter Usage

Measurement Type: Average

Measurement Dimension: Single

Description: Average Diameter ingress message processing rate of P-DRA during the collection interval.

Collection Interval: 5 min

Peg Condition: This peg is periodically updated based on average rate of the Diameter ingress messages being processed by P-DRA calculated over the collection interval.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraMsgRatePeak

Measurement Group: P-DRA Diameter Usage

Measurement Type: Max

Measurement Dimension: Single

Description: Peak Diameter ingress message processing rate of P-DRA during the collection interval.

Collection Interval: 5 min

Peg Condition: This peg is periodically updated based on maximum rate of the Diameter ingress messages being processed by P-DRA calculated over the collection interval.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraRarGxMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of RAR messages received by PDRA for Gx interface,

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives a RAR message for Gx interface.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraRarGxpMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime RAR messages processed by P-DRA.

Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime RAR message is processed by P-DRA.

Measurement Scope: All

Recovery:

No action required.

RxPdraRarRxMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of RAR messages received by PDRA for Rx interface.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented each time the application receives a RAR message for Rx interface.

Measurement Scope: All

Recovery:

No action necessary.

RxPdraStrMsgs

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of STR messages received by PDRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented per interface each time the application receives a STR message.

Measurement Scope: All

Recovery:

No action necessary.

TxPdraGxRarQuery

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx RAR messages initiated by P-DRA for the purposes of querying for session existence at the policy client.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a P-DRA DA-MP server sends a P-DRA initiated RAR request to a policy client for the purpose of querying the policy client for session existence.

Measurement Scope: All

Recovery:

1. If this value is consistently non-zero, it may indicate that the stale session timing is configured to be too short. The stale session timer for a given session is configured in **Policy DRA** > **Configuration** > **Access Point Names** if the session is associated with a configured APN, or **Policy DRA** > **Configuration** > **Network-Wide Options** if the session is not associated with an APN, or associated with an APN that is not configured.
2. If the problem persists, contact the *Customer Care Center*.

TxPdraGxRarRelease

Measurement Group: P-DRA Diameter Usage

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Gx RAR requests initiated by P-DRA for the purpose of releasing a session as a result of an error in the P-DRA.

Collection Interval: 5 min

Peg Condition: The measurement shall be pegged each time a P-DRA DA-MP server sends a P-DRA initiated RAR request to a policy client for the purpose of releasing a session due to an error in the P-DRA

Measurement Scope: All

Recovery:

1. Check **Alarms & Events** > **View History GUI**for pSBR event *22711 - Policy SBR Database Error* for more details about the possible cause of the error.
2. Contact the *Customer Care Center* for support as needed.

P-DRA Diameter Exception measurements

The P-DRA Diameter Exception measurement report contains measurements that provide performance information that is specific to the P-DRA Diameter protocol.

Table 62: P-DRA Diameter Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxBindCapPcrfPoolNotMapped	Number of binding capable session initiation requests that were destined for a PCRF Pool or Sub-Pool for which no PRT table was configured	5 min

Measurement Tag	Description	Collection Interval
RxBindCapUnknownApn	Number of binding capable session initiation requests containing an unconfigured APN	5 min
RxBindCapMissingApn	Number of binding capable session initiation requests containing no APN	5 min
RxBindDepUnknownApn	Number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing an unconfigured APN	5 min
RxBindDepMissingApn	Number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing no APN	5 min
RxBindCapUnknownPcrf	Number of binding capable session initiation answers coming from an unconfigured PCRF	5 min
RxPdraRequestProtocolErr	Number of invalid Request messages received from DRL. Invalid request message includes - unsupported command codes, unsupported application Id, missing or invalid AVPs.	5 min
RxStackEventDiscardedCaFailure	Number of stack events discarded by ComAgent due to ComAgent failures	5 min
TxAaxMsgDiscardedDueToDrlQueueFull	Number of AAR/AAA messages discarded by P-DRA due to DRL queue being full.	5 min
TxAsxMsgDiscardedDueToDrlQueueFull	Number of ASR messages discarded by P-DRA due to DRL queue being full.	5 min
TxCcxMsgDiscardedDueToDrlQueueFull	Number of CCR/CCA messages discarded by P-DRA due to DRL queue being full.	5 min
TxPdraAnswersGeneratedForDiameterErr	Number of Diameter answers generated by P-DRA due to error in received Diameter messages from DRL.	5 min
TxPdraAnswersGeneratedForPsrbErrResp	Number of Diameter Answer messages generated by P-DRA because of pSBR stack event error response.	5 min
TxPdraErrAnsGeneratedCAFailure	Number of Diameter answers generated by P-DRA due to ComAgent failure.	5 min

Measurement Tag	Description	Collection Interval
TxGxpCcxMsgDiscardedDrlQueueFull	Number of Gx-Prime CCR/CCA messages discarded by P-DRA due to the DRL queue being full.	5 min
TxRaxMsgDiscardedDueToDrlQueueFull	Number of RAR/RAA messages discarded by P-DRA due to DRL queue being full.	5 min
TxStxMsgDiscardedDueToDrlQueueFull	Number of STR/STA messages discarded by P-DRA due to DRL queue being full.	5 min

RxBindCapPcrfPoolNotMapped

Measurement Group: P-DRA Diameter Exception

Description: The number of binding capable session initiation requests that were destined for a PCRF Pool or Sub-Pool for which no PRT table was configured.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval: 5 min

Peg Condition: Each time a new binding attempt is supposed to be routed to a PCRF Pool or Sub-Pool for which no PRT table is configured at the site where the routing is occurring.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which a PCRF Pool or Sub-Pool has been configured for use at the NOAMP, but no PRT table has been configured at one or more sites to route requests to that PCRF Pool or Sub-Pool. Consider whether a PRT table should be configured at the Network Element to which this measurement applies
2. Contact the *Customer Care Center*.

RxBindCapUnknownApn

Measurement Group: P-DRA Diameter Exception

Description: The number of binding capable session initiation requests containing an unconfigured APN.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval: 5 min

Peg Condition: Each time a binding capable session initiation request is received containing an APN that is not configured at the Policy DRA NOAMP.

Note: This condition also causes *22730 - Policy DRA Configuration Error* to be asserted.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which binding capable session initiation request are being received from unknown APN values. Each binding capable session initiation request containing an unconfigured APN is rejected using the Missing Or Unconfigured APN error condition.
2. Contact the *Customer Care Center*.

RxBindCapMissingApn

Measurement Group: P-DRA Diameter Exception

Description: The number of binding capable session initiation requests containing no APN.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval: 5 min

Peg Condition: Each time a binding capable session initiation request is received containing no APN (i.e. no Called-Station-ID AVP).

Note: This condition also causes *22730 - Policy DRA Configuration Error* to be asserted.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which binding capable session initiation request are being received with no APN value. Each binding capable session initiation request containing a missing APN is rejected using the Missing Or Unconfigured APN error condition.
2. Contact the *Customer Care Center*.

RxBindDepUnknownApn

Measurement Group: P-DRA Diameter Exception

Description: The number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing an unconfigured APN.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval: 5 min

Peg Condition: Each time an attempt is made to find a binding using either IMSI or MSISDN, but the binding dependent session initiation request contains an APN that is not configured at the Policy DRA NOAMP. If both IMSI and MSISDN are configured in the binding key priority table, this measurement can be incremented twice for one binding dependent session initiation request.

Note: This condition also causes *22730 - Policy DRA Configuration Error* to be asserted.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which the binding key priority is configured to use IMSI, MSISDN, or both, but the binding dependent session initiation request has an APN value that is not configured. This condition causes binding correlation to fail for the MSISDN or IMSI key types. If no other key is present and configured for correlation, the request is rejected using the Binding Not Found error condition.
2. Contact the *Customer Care Center*.

RxBindDepMissingApn

Measurement Group: P-DRA Diameter Exception

Description: The number of attempts to correlate a binding dependent session initiation request using a non-specific binding correlation key (i.e. IMSI or MSISDN), but containing no APN

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval: 5 min

Peg Condition: Each time an attempt is made to find a binding using either IMSI or MSISDN, but the binding dependent session initiation request contains no APN. If both IMSI and MSISDN are configured in the binding key priority table, this measurement can be incremented twice for one binding dependent session initiation request.

Note: This condition also causes *22730 - Policy DRA Configuration Error* to be asserted.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which the binding key priority is configured to use IMSI, MSISDN, or both, but the binding dependent session initiation request has no APN value. This condition causes binding correlation to fail for the MSISDN or IMSI key types. If no other key is present and configured for correlation, the request is rejected using the Binding Not Found error condition.
2. Contact the *Customer Care Center*.

RxBindCapUnknownPcrf

Measurement Group: P-DRA Diameter Exception

Description: The number of binding capable session initiation answers coming from an unconfigured PCRF.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval: 5 min

Peg Condition: Each time a binding capable session initiation answer for a new binding is received from a PCRF that is not configured at the Policy DRA SOAM.

Note: This condition also causes *22730 - Policy DRA Configuration Error* to be asserted.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement represents an exception condition in which binding capable session initiation answers for new bindings are being received from unknown PCRF FQDNs. When this occurs, the binding capable session answered by the unconfigured PCRF is torn down by an RAR containing a Session-Release-Cause AVP send from the Policy DRA.
2. Refer to *22730 - Policy DRA Configuration Error* for further information.
3. Contact the *Customer Care Center*.

RxPdraRequestProtocolErr

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of invalid Request messages received from DRL. Invalid request message includes - unsupported command codes, unsupported application Id, missing or invalid AVPs. The AARs without Dest-Host AVP are still valid AARs and shall be pegged.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time an invalid diameter request message is received by P-DRA.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center* for assistance.

RxStackEventDiscardedCaFailure

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of stack events discarded by ComAgent due to ComAgent failure.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a stack event is discarded by ComAgent due to a ComAgent failure as indicated by a returned stack event error code of all available error codes.

Measurement Scope: All

Recovery:

1. Check ComAgent event *19832 - Communication Agent Reliable Transaction Failed* and ComAgent measurements *CAHSTxDscrdCongSR*, *CAHSTxDscrdUnkwnRsrc*, and *CAHSTxDscrdIntErrSR* for detailed error causes.
2. If the problem persists, contact the *Customer Care Center* for assistance.

TxAaxMsgDiscardedDueToDrlQueueFull

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of AAR/AAA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a AAR/AAA message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

No action required.

TxAsxMsgDiscardedDueToDrlQueueFull

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ASR messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a ASR message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

No action required.

TxCcxMsgDiscardedDueToDrlQueueFull

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of CCR/CCA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a CCR/CCA message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

No action required.

TxPdraAnswersGeneratedForDiameterErr

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Diameter answers generated by P-DRA due to error in received Diameter messages from DRL.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a diameter answer message is generated by P-DRA due to error in received Diameter messages from DRL.

The errors encountered may be:

- Diameter protocol errors
- P-DRA application specific errors due to absence of some optional AVP(s) in the Diameter request

Measurement Scope: All

Recovery:

No action required.

TxPdraAnswersGeneratedForPsbrErrResp

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Diameter Answer messages generated by P-DRA because of pSBR stack event error response.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a diameter answer message is generated by P-DRA because of pSBR stack event error response.

Measurement Scope: All

Recovery:

No action required.

TxPdraAnswersGeneratedPcrfConfigErr

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Diameter Answers generated by P-DRA due to configuration errors when processing binding capable session initiation requests.

Collection Interval: 5 min

Peg Condition: This measurement is pegged each time when P-DRA generates an error Anser in processing a binding capable session initiation request due to

- No PCRF being configured at the site where the request is processed OR
- No PCRF ID being found in PCRF table OR
- The APN contained in the request message not configured.

The measurement is pegged also each time when P-DRA generates an error Answer in processing a binding dependent session initiation request if the APN in te request is not configured in the Policy DRA and the site is configured to correlate on IMSI, MSISDN, or both and no other binding correlation key is successfully used for correlation.

Note: In binding dependent request cases, this measurement is raised only when the Binding Not Found condition applies, the APN is unconfigured, and an IMSI or MSISDN was used as a possible correlation key.

Measurement Scope: All

Recovery:

1. Check the P-DRA System OAM GUI Main Menu: **Policy DRA** > **Configuration** > **PCRFs** to ensure PCRFs are configured properly.
2. If there is an unconfigured PCRF, it means that the binding capable session initiation request was routed to a PCRF that is not configured in **Policy DRA** > **Configuration** > **PCRFs** at the site where the request was received. This indicates a mismatch between the PCRF's configuration and the routing configuration. If the PCRF is a valid choice for the request, configure the PCRF in **Policy DRA** > **Configuration** > **PCRFs**. If the PCRF is not valid for the request, correct the routing table or tables that included the PCRF.

   See also *RxBindCapUnknownPcrf*.
3. If there is an unconfigured APN and if the APN string is valid, configure the APN at the NOAMP using the **Policy DRA** > **Configuration** > **Access Point Names** screen. If the APN string is not valid, investigate the policy client to determine why it is sending policy session initiation requests using the invalid APN.

   See also *RxBindCapUnknownApn* and *RxBindDepUnknownApn*.
4. If there is a missing APN, investigate the policy client to determine why it is sending policy session initiation requests with no APN.

   See also *RxBindCapMissingApn* and *RxBindDepMissingApn*
5. If there are no PCRFs configured, configure PCRFs at the SOAM GUI for the site using **Policy DRA** > **Configuration** > **PCRFs**.
6. If needed, contact the *Customer Care Center* for further assistance.

TxPdraErrAnsGeneratedCAFailure

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Diameter answers generated by P-DRA due to ComAgent failure.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a diameter answer message is generated by P-DRA due to comagent routing failure.

Measurement Scope: All

Recovery:

No action required.

TxGxpCcxMsgDiscardedDrlQueueFull

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CCR/CCA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime CCR/CCA message is discarded by the P-DRA application because DRL queue is full.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center*.

TxRaxMsgDiscardedDueToDrlQueueFull

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of RAR/RAA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a RAR/RAA message is discarded by the application because DRL queue is full. The measurement shall be incremented by one each time a CCR/CCA message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

No action required.

TxStxMsgDiscardedDueToDrlQueueFull

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Description: Number of STR/STA messages discarded by P-DRA due to DRL queue being full.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a STR/STA message is discarded by the application because DRL queue is full.

Measurement Scope: All

Recovery:

No action required.

P-DRA Congestion Exception measurements

The P-DRA Congestion Exception measurement report contains measurements that provide performance information that is specific to the P-DRA Diameter protocol.

Table 63: P-DRA Congestion Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxAarMsgDiscardedDueToCongestion	Number of AAR messages discarded by P-DRA due to congestion.	5 min
RxAsrMsgDiscardedDueToCongestion	Number of ASR messages discarded by P-DRA due to P-DRA congestion.	5 min
RxCcrMsgDiscardedDueToCongestion	Number of CCR messages discarded by P-DRA due to congestion.	5 min
RxGxpCcrMsgDiscardedDueToCongestion	Number of Gx-Prime CCR messages discarded by P-DRA due to P-DRA internal congestion.	5 min
RxRarMsgDiscardedDueToCongestion	Number of RAR messages discarded by P-DRA due to congestion.	5 min
RxStrMsgDiscardedDueToCongestion	Number of STR messages discarded by P-DRA due to congestion.	5 min

RxAarMsgDiscardedDueToCongestion

Measurement Group: P-DRA Congestion Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of AAR messages discarded by P-DRA due to congestion.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time an AAR message is discarded by P-DRA due to congestion.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center* for assistance.

RxAsrMsgDiscardedDueToCongestion

Measurement Group: P-DRA Congestion Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ASR messages discarded by P-DRA due to P-DRA congestion.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time an ASR message is discarded by P-DRA due to congestion.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center* for assistance.

RxCcrMsgDiscardedDueToCongestion

Measurement Group: P-DRA Congestion Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of CCR messages discarded by P-DRA due to congestion.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time a CCR message is discarded by P-DRA due to congestion.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center* for assistance.

RxGxpCcrMsgDiscardedDueToCongestion

Measurement Group: P-DRA Diameter Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of Gx-Prime CCR messages discarded by P-DRA due to P-DRA internal congestion.

Collection Interval: 5 min

Peg Condition: Each time a Gx-Prime CCR message is discarded by the P-DRA application due to P-DRA internal congestion.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center* for assistance.

RxRarMsgDiscardedDueToCongestion

Measurement Group: P-DRA Congestion Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of RAR messages discarded by P-DRA due to congestion.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time an RAR message is discarded by P-DRA due to congestion.

Measurement Scope: Network, NE, Server

Recovery:

Contact the *Customer Care Center* for assistance.

RxStrMsgDiscardedDueToCongestion

Measurement Group: P-DRA Congestion Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of STR messages discarded by P-DRA due to congestion.

Collection Interval: 5 min

Peg Condition: The measurement shall be incremented by one each time an STR message is discarded by P-DRA due to congestion.

Measurement Scope: All

Recovery:

Contact the *Customer Care Center* for assistance.

pSBR Binding Performance measurements

The pSBR Binding Performance measurement report contains measurements that provide performance information that is specific to the pSBR Binding Database.

Table 64: pSBR Binding Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
PsbrNewBindingsCreated	The number of new bindings created.	5 min
PsbrUpdatedBindings	The number of existing bindings updated but not deleted	5 min
PsbrBindTermByAscSess	The number bindings (final) terminated due to termination of all associated sessions.	5 min
PsbrAltKeyCreated	The number of alternate key records created.	5 min
PsbrAltKeyDel	The number of alternate key records removed.	5 min
PsbrMaxBindingAgeAtTerm	The average binding (final) age when binding is terminated due to termination of all associated sessions	5 min
PsbrAvgBindingAgeAtTerm	The maximum binding (final) age when binding is terminated due to termination of all associated sessions.	5 min
PsbrAvgBindingDbRead	The average rate of Binding database reads per second	5 min
PsbrMaxBindingDbRead	The maximum rate of Binding database reads	5 min
PsbrAvgBindingDbWrite	The average rate of Binding database writes per second	5 min
PsbrMaxBindingDbWrite	The maximum rate of Binding database writes	5 min
PsbrEarlySlaveBindingsCreated	The number of binding capable session initiation requests that	5 min

Measurement Tag	Description	Collection Interval
	were treated as slaves of an existing early binding	
PsbrFinalBindingsFollowed	The number of binding capable session initiation requests for which an existing final binding existed	5 min
PsbrSlavePollingContinue	The number of early binding polling attempts for which the poller was instructed to continue polling	5 min
PsbrSlavePollingRouteToPcrf	The number of early binding polling attempts for which the poller was instructed to route to a final binding	5 min

PsbrNewBindingsCreated

Measurement Group: pSBR Binding Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of new bindings created.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a new binding is created.

Measurement Scope: Place Association

Recovery:

No action necessary.

PsbrUpdatedBindings

Measurement Group: pSBR Binding Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of existing bindings updated but not deleted, i.e. the Session Reference removed is not the last one

Collection Interval: 5 min

Peg Condition: This peg is updated whenever an existing binding is updated.

Measurement Scope: Place Association

Recovery:

No action necessary.

PsbrBindTermByAscSess

Measurement Group: pSBR Binding Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number bindings (final) terminated due to termination of all associated sessions.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a binding is terminated due to termination of all associated sessions.

Measurement Scope: Place Association

Recovery:

No action necessary.

PsbrAltKeyCreated

Measurement Group: pSBR Binding Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of alternate key records created.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever an alternate key record is created.

Measurement Scope: Place Association

Recovery:

No action necessary.

PsbrAltKeyDel

Measurement Group: pSBR Binding Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of alternate key records removed.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever an alternate key record is deleted.

Measurement Scope: Place Association

Recovery:

No action necessary.

PsbrMaxBindingAgeAtTerm

Measurement Group: pSBR Binding Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The maximum binding (final) age when binding is terminated due to termination of all associated sessions.

Collection Interval: 5 min

Peg Condition: The time interval starts when the binding becomes final and stops when binding is terminated due to termination of all associated sessions.

Measurement Scope: Place Association

Recovery:

No action necessary.

PsbrAvgBindingAgeAtTerm

Measurement Group: pSBR Binding Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average binding (final) age when binding is terminated due to termination of all associated sessions.

Collection Interval: 5 min

Peg Condition: The time interval starts when the binding becomes final and stops when binding is terminated due to termination of all associated sessions.

Measurement Scope: All

Recovery:

No action necessary.

PsbrAvgBindingDbRead

Measurement Group: pSBR Binding Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average rate of Binding database reads per second

Collection Interval: 5 min

Peg Condition: It is calculated based on the total number of sampled binding database reads during the collection interval.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMaxBindingDbRead

Measurement Group: pSBR Binding Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The maximum rate of Binding database reads

Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with the average binding database reads, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: All

Recovery:

No action necessary.

PsbrAvgBindingDbWrite

Measurement Group: pSBR Binding Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average rate of Binding database writes per second

Collection Interval: 5 min

Peg Condition: It is calculated based on the total number of sampled binding database writes during the collection interval.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMaxBindingDbWrite

Measurement Group: pSBR Binding Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The maximum rate of Binding database writes

Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with the average binding database writes, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: All

Recovery:

No action necessary.

PsbrEarlySlaveBindingsCreated

Event Group: pSBR Binding Performance

Description: The number of binding capable session initiation requests that were treated as slaves of an existing early binding.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time a binding capable session initiation request is received and all of the following conditions are true:

- The CCR-I matches an existing binding that is in the Early state (i.e. there exists an EarlyMaster sessionRef for the IMSI and APN, or IMSI and PCRF Pool)
- The existing EarlyMaster sessionRef has not been in existence for longer than the Maximum Early Binding Lifetime configured in **Policy DRA** > **Configuration** > **Network-Wide Options**
- PCRF Pooling is Enabled

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the frequency at which the early binding mechanism is being exercised.
2. Contact the *Customer Care Center*.

PsbrFinalBindingsFollowed

Event Group: pSBR Binding Performance

Description: A count fo the number of binding capable session initiation requests that matched a final binding and were routed using the bound PCRF.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time a binding capable session initiation request is received and all of the following conditions are true:

- The CCR-I matches an existing binding that is in the Final state (i.e. there exists a Final sessionRef for the IMSI and APN, or IMSI and PCRF Pool)
- PCRF Pooling is Enabled

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the frequency at which binding capable session initiation requests are routed according to existing bindings.
2. Contact the *Customer Care Center*.

PsbrSlavePollingContinue

Measurement Group: pSBR Binding Performance

Description: A count of the number of early binding polling attempts for which the poller was instructed to continue polling.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time an Early Binding Slave session polls the Early Binding Master and all of the following conditions are true:

- The Early Binding Master sessionRef still exists in the binding database and is in the EarlyMaster state.
- The Early Binding Slave sessionRef still exists in the binding database
- The Early Binding Master sessionRef has not been in existence for longer than the Maximum Early Binding Lifetime
- PCRF Pooling is Enabled

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the frequency at slave pollers are asked to continue polling. If this value is equal to or higher than the PsbrEarlySlaveBindingsCreated, the Early Binding Polling Interval configured in **Policy DRA** > **Configuration** > **Network-Wide Options** may be set to a duration too short, causing unnecessary polling attempts. If this value is very low relative to the *PsbrEarlySlaveBindingsCreated*, the Early Binding Polling Interval may be set to a duration too long, causing unnecessary latency for slave sessions.
2. Contact the *Customer Care Center*.

PsbrSlavePollingRouteToPcrf

Measurement Group: pSBR Binding Performance

Description: A count of the number of early binding polling attempts for which the poller was instructed to route the request to a bound PCRF.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time an Early Binding Slave session polls the Early Binding Master and all of the following conditions are true:

- The Early Binding Master sessionRef still exists in the binding database and is in the Final state.
- The Early Binding Slave sessionRef still exists in the binding database
- PCRF Pooling is Enabled

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the Early Binding Slave sessions whose master sessionRefs became Final and were therefore routed using the bound PCRF. If this value is lower than the *PsbrEarlySlaveBindingsCreated* value, check the pSBR Binding Exception measurement report for measurement *PsbrSlavePollingFail*.
2. Contact the *Customer Care Center*.

pSBR Session Performance measurements

The pSBR Binding Performance measurement report contains measurements that provide performance information that is specific to the pSBR Session Database.

Table 65: pSBR Session Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
PsbrSessionsCreated	The number of new sessions created.	5 min
PsbrSessionsRefresh	The number of existing sessions refreshed.	5 min
PsbrSessionsDeleted	The number of sessions removed.	5 min
PsbrAvgSessionAgeTermPerAPN	The average time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.	5 min
PsbrMaxSessionAgeTermPerAPN	The maximum time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.	5 min
PsbrAvgSessionDbRead	The average rate of Session database reads per second	5 min

Measurement Tag	Description	Collection Interval
PsbrMaxSessionDbRead	At the end of each sample period associated with the average session database reads , if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.	5 min
PsbrAvgSessionDbWrite	The average rate of session database writes per second	5 min
PsbrMaxSessionDbWrite	The maximum rate of session database writes	5 min

PsbrSessionsCreated

Measurement Group: pSBR Session Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of new sessions created.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a new session is created.

Measurement Scope: All

Recovery:

No action necessary.

PsbrSessionsRefresh

Measurement Group: pSBR Session Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of existing sessions refreshed.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever an existing session is refreshed.

Measurement Scope: All

Recovery:

No action necessary.

PsbrSessionsDeleted

Measurement Group: pSBR Session Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of sessions removed.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a session is deleted.

Measurement Scope: All

Recovery:

No action necessary.

PsbrAvgSessionAgeTermPerAPN

Measurement Group: pSBR Session Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.

Collection Interval: 5 min

Peg Condition: The time interval starts when a session record is created as a result of createSession stack event and stops when the session record is terminated successfully as a result of removeSession stack event

Measurement Scope: All

Recovery:

No action necessary.

PsbrMaxSessionAgeTermPerAPN

Measurement Group: pSBR Session Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The maximum time interval (in hours) per APN between the time when a session record is created and the time when it is successfully terminated.

Collection Interval: 5 min

Peg Condition: The time interval starts when a session record is created as a result of createSession stack event and stops when the session record is terminated successfully as a result of removeSession stack event

Measurement Scope: All

Recovery:

No action necessary.

PsbrAvgSessionDbRead

Measurement Group: pSBR Session Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average rate of Session database reads per second

Collection Interval: 5 min

Peg Condition: It is calculated based on the total number of sampled session database reads during the collection interval.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMaxSessionDbRead

Measurement Group: pSBR Session Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The maximum rate of Session database reads

Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with the average session database reads, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value

Measurement Scope: All

Recovery:

No action necessary.

PsbrAvgSessionDbWrite

Measurement Group: pSBR Session Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average rate of session database writes per second

Collection Interval: 5 min

Peg Condition: It is calculated based on the total number of sampled session database writes during the collection interval.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMaxSessionDbWrite

Measurement Group: pSBR Session Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The maximum rate of session database writes

Collection Interval: 5 min

Peg Condition: At the end of each sample period associated with the average session database writes, if the maximum value exceeds the current value of this measurement, then the measurement will be updated with the current sample periods value.

Measurement Scope: All

Recovery:

No action necessary.

pSBR Binding Exception measurements

The pSBR Binding Exception measurement report contains measurements that provide performance information that is specific to the pSBR Binding Database.

Table 66: pSBR Binding Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
PsbrCreateBindDbErr	The number of errors creating a binding record.	5 min
PsbrUpdateBindDbErr	The number of errors updating a binding record.	5 min
PsbrRemoveBindDbErr	The number of errors removing a suspect binding record	5 min
PsbrCreateAltKeyDbErr	The number of errors creating an alternate key record.	5 min
PsbrRemoveAltKeyDbErr	The number of errors removing an alternate key record.	5 min

Measurement Tag	Description	Collection Interval
PsbrFindBindDbErr	The number of errors when encountered for finding a binding record.	5 min
PsbrEarlyTooLongSrRemoved	The number of sessionRefs found to be in the EarlyMaster or EarlySlave state for too long	5 min
PsbrSlavePollingFail	The number of binding capable session initiation requests that were not routed due to polling failures	5 min
PsbrSuspectSrRemoved	The number of binding sessionRefs removed as a result of the Suspect Binding mechanism	5 min

PsbrCreateBindDbErr

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of errors creating a binding record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever there is an error in creating a binding record.

Measurement Scope: All

Recovery:

No action necessary.

PsbrUpdateBindDbErr

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of errors updating a binding record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever there is an error in updating a binding record.

Measurement Scope: All

Recovery:

No action necessary.

PsbrRemoveBindDbErr

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of errors removing a suspect binding record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever there is an error in removing a suspect binding record.

Measurement Scope: All

Recovery:

No action necessary.

PsbrCreateAltKeyDbErr

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of errors creating an alternate key record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever there is an error in creating an alternate key record.

Measurement Scope: All

Recovery:

No action necessary.

PsbrRemoveAltKeyDbErr

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of errors removing an alternate key record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever there is an error in removing an alternate key record.

Measurement Scope: All

Recovery:

No action necessary.

PsbrFindBindDbErr

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of errors when encountered for finding a binding record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever there is an error in finding a binding record.

Measurement Scope: All

Recovery:

No action necessary.

PsbrEarlyTooLongSrRemoved

Event Group: pSBR Binding Exception

Description: A count of the number of sessionRefs found to be in the EarlyMaster or EarlySlave state for longer than the Maximum Early Binding Lifetime.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time sessionRef is discovered that has been in an early state (i.e. EarlyMaster or EarlySlave) for longer than the Maximum Early Binding Lifetime and the following conditions are true:

- PCRF Pooling is Enabled AND
  - A binding capable session initiation request is received that matches an existing binding and the binding has been in the EarlyMaster state for longer than the Maximum Early Binding Lifetime OR
  - A binding capable session initiation request is received and no slots are available for new sessionRefs, but at least one sessionRef has been in the EarlySlave state for longer than the Maximum Early Binding Lifetime OR
  - A slave session polls a master sessionRef that has been in the EarlyMaster state for longer than the Maximum Early Binding Lifetime

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the frequency at which binding sessionRefs are discovered in an early state for longer than expected. This unexpected condition could occur if the Maximum Early Binding Lifetime value is configured to be nearly equal to or shorter than the Diameter transaction timer. It could also occur if the binding pSBR was in congestion and load shedding prevented the session from being transitioned from the early state to a final state. In either case the "stuck" sessionRef is removed, preventing it from disrupting further signaling.

2. Contact the *Customer Care Center*.

PsbrSlavePollingFail

Event Group: pSBR Binding Exception

Description: A count of the number of binding capable session initiation requests that were not routed to polling failures. This includes the following: slave sessionRef not found, master sessionRef, master sessionRef found, but existed for longer than the Maximum Early Binding Lifetime.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time an Early Binding Slave session polls the Early Binding master and the following conditions are met:

- PCRF Pooling is Enabled AND
  - The Early Binding Master sessionRef no longer exists in the binding database OR
  - The Early Binding Slave sessionRef no longer exists in the binding database OR
  - The Early Binding Master sessionRef exists in the binding database in the EarlyMaster state, but has been in existence for longer than the Maximum Early Binding Lifetime

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the Early Binding Slave sessions whose polling attempts did NOT result in a final binding to route towards. Each time this measurement is pegged, P-DRA generates an error answer message using the Binding Found But Unable To Route Diameter result code. The Error-Message AVP contains a 3-digit code that indicates the specific reason for the failure.
2. Contact the *Customer Care Center*.

PsbrSuspectSrRemoved

Measurement Group: pSBR Binding Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: A count of the number of binding sessionRefs removed as a result of the Suspect Binding mechanism.

Collection Interval 5 min

Peg Condition: Each time a binding sessionRef is removed by the suspect binding mechanism (i.e. due to inaccessability of a PCRF for more than 30 seconds while signaling attempts are being performed).

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the number of binding sessionRefs that were automatically removed from the Policy DRA binding database as a result of continued inability to route binding capable session initiation requests to a given PCRF.
2. Contact the *Customer Care Center*.

pSBR Session Exception measurements

The pSBR Session Exception measurement report contains measurements that provide performance information that is specific to the pSBR Session Database.

Table 67: pSBR Session Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
PsbrCreateSessDbErr	The number of errors creating a session record.	5 min
PsbrRefreshSessDbErr	The number of errors refreshing a session record.	5 min
PsbrRemSessDbErr	The number of errors terminating a session record.	5 min
PsbrFindSessionDbErr	The number of errors when encountered for finding a session record.	5 min
PsbrRemSessRarAttempts	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.	5 min

PsbrCreateSessDbErr

Measurement Group: pSBR 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:

No action necessary.

PsbrRefreshSessDbErr

Measurement Group: pSBR 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:

No action necessary.

PsbrRemSessDbErr

Measurement Group: pSBR 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:

No action necessary.

PsbrFindSessDbErr

Measurement Group: pSBR 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:

No action necessary.

PsbrRemSessRarAttempts

Measurement Group: pSBR 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.

pSBR Audit measurements

The pSBR Audit measurement report contains measurements that provide performance information that is specific to the pSBR Binding Database.

Table 68: pSBR Audit Measurement Report Fields

Measurement Tag	Description	Collection Interval
PsbrImsiAuditDbErr	The number of ImsiAnchorKey audit failures due to DB errors	5 min
PsbrMsisdnAuditDbErr	The number of MsidnAlternateKey audit failures due to DB error.	5 min
PsbrIpv4AuditDbErr	The number of Ipv4AlternateKey audit failures due to DB error.	5 min
PsbrIpv6AuditDbErr	The number of Ipv6AlternateKey audit failures due to DB error.	5 min
PsbrSessionRecsAudited	The number of Session Records audited during the reporting interval.	5 min
PsbrExpiredSessionsFound	The number of Expired Session Records found by audit during the reporting interval.	5 min
PsbrImsiRecsAudited	The number of IMSI Anchor Key Records audited during the reporting interval.	5 min
PsbrStaleSessionRemoved	The number of stale session records that are terminated by audit.	5 min
PsbrIpv4RecsAudited	The number of IPv4 Alternate Key Records audited during the reporting interval	5 min

Measurement Tag	Description	Collection Interval
PsbrIpv4RecsRemoved	The number of IPv4 Alternate Key Records removed by audit during the reporting interval.	5 min
PsbrIpv6RecsAudited	The number of IPv6 Alternate Key Records audited during the reporting interval.	5 min
PsbrSessionAuditDbErr	The number of Session audit failures due to DB error.	5 min
PsbrSessionRefAuditDbErr	The number of SessionRef audit failures due to DB errors.	5 min
PsbrImsiAuditCaErr	The number of ImsiAnchorKey audit failures due to ComAgent errors	5 min
PsbrMsisdnAuditCongErr	The number of MsidnAlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.	5 min
PsbrIpv4AuditCaErr	The number of Ipv4AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.	5 min
PsbrIpv6AuditCaErr	The number of Ipv6AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.	5 min
PsbrIpv6RecsRemoved	The number of IPv6 Alternate Key Records removed by audit during the reporting interval.	5 min
PsbrMsisdnRecsAudited	The number of MSISDN Alternate Key Records audited during the reporting interval.	5 min
PsbrMsisdnRecsRemoved	The number of MSISDN Alternate Key Records removed by audit during the reporting interval.	5 min
PsbrImsiRecsRemoved	The number of IMSI Anchor Key Records removed by audit during the reporting interval.	5 min
PsbrImsiSrRemovedByAudit	The number of IMSI binding sessionRefs removed as a result of the Binding Audit mechanism	5 min
PsbrMsisdnSrRemovedByAudit	The number of MSISDN binding sessionRefs removed as a result of the Binding Audit mechanism	5 min

PsbrImsiAuditDbErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ImsiAnchorKey audit failures due to DB errors

Collection Interval: 5 min

Peg Condition: This peg is updated whenever an ImsiAnchorKey audit fails due to a DB error.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMsisdnAuditDbErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of MsidnAlternateKey audit failures due to DB error.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a MsidnAlternateKey audit fails due to DB error.

Measurement Scope: All

Recovery:

No action necessary.

PsbrIpv4AuditDbErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Ipv4AlternateKey audit failures due to DB error.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a Ipv4AlternateKey audit fails due to a DB error.

Measurement Scope: All

Recovery:

No action necessary.

PsbrIpv6AuditDbErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Ipv6AlternateKey audit failures due to DB error.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a Ipv6AlternateKey audit fails due to a DB error.

Measurement Scope: All

Recovery:

No action necessary.

PsbrSessionRecsAudited

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Session Records audited during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time a Session record is audited.

Measurement Scope: All

Recovery:

No action necessary.

PsbrExpiredSessionsFound

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Expired Session Records found by audit during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time a Session record is audited and found to be stale.

Measurement Scope: All

Recovery:

No action necessary.

PsbrImsiRecsAudited

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of IMSI Anchor Key Records audited during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an ImsiAnchorKey record is audited.

Measurement Scope: All

Recovery:

No action necessary.

PsbrStaleSessionRemoved

Measurement Group: pSBR Session Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of stale session records that are terminated by audit.

Collection Interval: 5 min

Peg Condition: Every time a session record is audited that finds a time out.

Measurement Scope: All

Recovery:

No action necessary.

PsbrIpv4RecsAudited

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of IPv4 Alternate Key Records audited during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an Ipv4AlternateKey record is audited.

Measurement Scope: All

Recovery:

No action necessary.

PsbrIpv4RecsRemoved

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of IPv4 Alternate Key Records removed by audit during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an Ipv4AlternateKey record is removed by audit.

Measurement Scope: All

Recovery:

No action necessary.

PsbrIpv6RecsAudited

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of IPv6 Alternate Key Records audited during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an Ipv6AlternateKey record is audited.

Measurement Scope: All

Recovery:

No action necessary.

PsbrSessionAuditDbErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Session audit failures due to DB error.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a Session audit fails due to DB error.

Measurement Scope: All

Recovery:

No action necessary.

PsbrSessionRefAuditDbErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of SessionRef audit failures due to DB errors.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a SessionRef audit fails due to DB error.

Measurement Scope: All

Recovery:

No action necessary.

PsbrImsiAuditCaErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of ImsiAnchorKey audit failures due to ComAgent errors

Collection Interval: 5 min

Peg Condition: This peg is updated whenever an ImsiAnchorKey audit fails due to ComAgent error.

Measurement Scope: All

Recovery:

1. Check ComAgent event *19832 - Communication Agent Reliable Transaction Failed* and ComAgent measurements *CAHSTxDscrdCongSR*, *CAHSTxDscrdUnkwnRsrc*, and *CAHSTxDscrdIntErrSR* for detailed error causes.
2. If the problem persists, contact the *Customer Care Center* for assistance.

PsbrMsisdnAuditCongErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of MsidnAlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.

Collection Interval: 5 min

Peg Condition: This peg is updated when a MsidnAlternateKey audit fails due to a ComAgent error.

Measurement Scope: All

Recovery:

1. Check ComAgent event *19832 - Communication Agent Reliable Transaction Failed* and ComAgent measurements *CAHSTxDscrdCongSR*, *CAHSTxDscrdUnkwnRsrc*, and *CAHSTxDscrdIntErrSR* for detailed error causes.
2. If the problem persists, contact the *Customer Care Center* for assistance.

PsbrIpv4AuditCongErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Ipv4AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a Ipv4AlternateKey audit fails due to ComAgent error.

Measurement Scope: All

Recovery:

1. Check ComAgent event *19832 - Communication Agent Reliable Transaction Failed* and ComAgent measurements *CAHSTxDscrdCongSR*, *CAHSTxDscrdUnkwnRsrc*, and *CAHSTxDscrdIntErrSR* for detailed error causes.
2. If the problem persists, contact the *Customer Care Center* for assistance.

PsbrIpv6AuditCongErr

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of Ipv6AlternateKey audit failures due to a ComAgent error condition when the pSBR sends findSessionRef stack event to the active pSBR for the sessionReference record.

Collection Interval: 5 min

Peg Condition: This peg is updated whenever a Ipv6AlternateKey audit fails due to ComAgent error.

Measurement Scope: All

Recovery:

1. Refer to ComAgent event *19832 - Communication Agent Reliable Transaction Failed* and ComAgent measurements *CAHSTxDscrdCongSR*, *CAHSTxDscrdUnkwnRsrc*, and *CAHSTxDscrdIntErrSR* for detailed error causes.
2. If the problem persists, contact the *Customer Care Center* for assistance.

PsbrIpv6RecsRemoved

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of IPv6 Alternate Key Records removed by audit during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an Ipv6AlternateKey record is removed by audit.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMsisdnRecsAudited

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of MSISDN Alternate Key Records audited during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an MsisdnAlternateKey record is audited.

Measurement Scope: All

Recovery:

No action necessary.

PsbrMsisdnRecsRemoved

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of MSISDN Alternate Key Records removed by audit during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an MsisdnAlternateKey record is removed by audit.

Measurement Scope: All

Recovery:

No action necessary.

PsbrImsiRecsRemoved

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of IMSI Anchor Key Records removed by audit during the reporting interval.

Collection Interval: 5 min

Peg Condition: This peg is incremented by one each time an ImsiAnchorKey record is removed by audit.

Measurement Scope: All

Recovery:

No action necessary.

PsbrImsiSrRemovedByAudit

Event Group: pSBR Audit

Description: A count of the number of IMSI binding sessionRefs removed by the binding audit.

Measurement Type: Simple

Measurement Dimension: Single

Collection Interval 5 min

Peg Condition: Each time the binding audit decides to remove an IMSI binding sessionRef due the following conditions:

- PCRF Pooling is Enabled AND
  - The binding sessionRef has been in the database for at least 30 seconds AND
  - The binding sessionRef has no corresponding session in the session database

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the number of IMSI bindings that for some reason were not removed when the associated Diameter session either failed or was terminated via signaling. This unexpected condition could occur if binding pSBR congestion load shedding prevented removal of the sessionRef from the binding record.
2. Contact the *Customer Care Center*.

PsbrMsisdnSrRemovedByAudit

Measurement Group: pSBR Audit

Measurement Type: Simple

Measurement Dimension: Single

Description: A count of the number of MSISDN binding sessionRefs removed by the binding audit.

Collection Interval 5 min

Peg Condition: Each time the binding audit decides to remove an MSISDN sessionRef because the binding sessionRef has no corresponding session in the session database.

Measurement Scope: Network Element, Server Group, Resource Domain, Place, Place Association

Recovery:

1. This measurement gives an indication of the number of MSISDN bindings that for some reason were not removed when the associated Diameter session either failed or was terminated via signaling. This unexpected condition could occur if binding pSBR congestion load shedding prevented removal of the sessionRef from the binding record.
2. Contact the *Customer Care Center*.

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.

Table 69: Peer Routing Rules Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxPeerAnswers	Number of routable Answer messages received from Peer-X	5 min
RxPeerRequests	Number of routable Request messages received from Peer-X	5 min
TxPeerAnswers	Number of routable Answer messages sent to Peer-X	5 min
TxPeerRequests	Number of routable Request messages sent to Peer-X	5 min

RxPeerAnswers

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:

No action required.

RxPeerRequests

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 an Request message event from DCL with a valid Transport Connection ID owned by Peer-X.

Measurement Scope: Server Group

Recovery:

No action required.

TxPeerAnswers

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 a Request message for Peer-X to DCL.

Measurement Scope: Server Group

Recovery:

No action required.

TxPeerRequests

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:

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.

Table 70: Peer Routing Rules Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxPrtSelected	Number of times that a peer routing rule from PRT-X was selected for routing a Request message.	5 min
RxRuleDuplicatePriority	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.	5 min
RxRuleFwdFailActionSendAns	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".	5 min
RxRuleFwdFailAll	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.	5 min
RxRuleSelected	Number of times that the Peer Routing Rule was selected for routing a Request message.	5 min

Measurement Tag	Description	Collection Interval
TxMsgPrtMarkedForCpy	Number of Request Messages set to a valid MCCS and marked for Message Copy	5 min

RxPrtSelected

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:

No action required.

RxRuleDuplicatePriority

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, contact the *Customer Care Center*.

RxRuleFwdFailActionSendAns

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:

No action required.

RxRuleFwdFailAll

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.

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: Server Group

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 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:

No action required.

TxMsgPrtMarkedForCpy

Measurement Group: Peer Routing Rules

Measurement Type: Simple

Measurement Dimension: Arrayed (by Peer Routing Rule ID)

Description: The 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.

Recovery:

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.

Table 71: Route List Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxRouteListFailure	Number of times that a Route List was selected for routing a Request message and the DSR was unable to successfully route the message.	5 min
RxRouteListSelected	Number of times the Route List was selected for routing a Request message.	5 min
RxRouteListUnavailable	Number of Request messages from a downstream peer that were rejected by a Local Node because the Route List selected had an "Operational Status" of "Unavailable".	5 min
TmRouteListOutage	Time duration that the Route List was unavailable during the measurement interval.	5 min

RxRouteListFailure

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 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: Server Group

Recovery:

1. Check the Route List settings using the **Diameter** > **Configuration** > **Route Lists** page.
2. Contact the *Customer Care Center* for assistance if needed.

RxRouteListSelected

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:

No action required.

RxRouteListUnavailable

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.

The Route List measurement is associated with the Route List selected for routing.

Measurement Scope: Server Group

Recovery:

1. The operation status of the Route List should be verified using the **Diameter** > **Maintenance** > **Route Lists** page.
2. Contact the *Customer Care Center* for assistance if needed.

TmRouteListOutage

Measurement Group: Route List

Measurement Type: Simple

Measurement Dimension: Arrayed (by Route List ID)

Description: 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.

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* is asserted.
2. Alarm *22053 - Route List Unavailable* 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* is asserted.
2. Alarm *22053 - Route List Unavailable* is cleared.

When a time duration interval completes, the time measured is added to the total measurement value.

Measurement Scope: Server Group

Recovery:

1. The operation status of the Route List should be verified using the **Diameter** > **Maintenance** > **Route Lists** page.
2. Contact the *Customer Care Center* 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.

Table 72: Routing Usage Measurement Report Fields

Measurement Tag	Description	Collection Interval
RxRoutedIntraMPAttempt	Number of attempts to route an ingress request message via intra-MP routing.	5 min
RxRoutedPeerDirect	Number of Request messages implicitly routed directly to a peer.	5 min
RxRoutedPeerRouteList	Number of Request messages implicitly routed to a peer via its alternate implicit route.	5 min
RxRoutedPrt	Number of Request messages routed using Peer Routing Rules.	5 min

RxRoutedIntraMPAttempt

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:

No action required.

RxRoutedPeerDirect

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:

No action required.

RxRoutedPeerRouteList

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:

No action required.

RxRoutedPrt

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:

No action required.

Server Exception measurements

Measurement Tag	Description	Collection Interval
EvError	Number of normal errors encountered	30 min
EvVital	Number of severe errors encountered	30 min

EvError

Measurement Group: Server Exception

Measurement Type: Simple

Description: The number of error trace conditions. This indicates that an expected but abnormal path was taken in the software, which warrants further investigation.

By default, error tracing is disabled. Non-zero values in this measurement indicate that something is occurring that would have generated an error trace, were error tracing enabled. These error trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

Contact the *Customer Care Center* for assistance if any unexpected non-zero values in this measurement occur.

EvVital

Measurement Group: Server Exception

Measurement Type: Simple

Description: The number of vital trace conditions encountered. A vital trace indicates that an unexpected path was taken in the software, which warrants further investigation. These vital trace conditions should not affect service; situations that are service affecting will be covered by Alarms or Events.

During application start-up and shutdown, vital traces are used to show details that can aid in debugging of initialization and shutdown problems. These traces are always enabled and cannot be turned off.

It is a VITAL error condition for any other instance.

Collection Interval: 30 min

Measurement Scope: NE, Server

Recovery:

Contact the *Customer Care Center* for assistance if any unexpected non-zero values in this measurement occur.

Session Binding Repository (SBR) Exception measurements

The "SBR Exception" measurement group is a set of measurements that provide information about exceptions and unexpected messages and events specific to the SBR application. Measurements such as the following are included in this group.

Table 73: SBR Exception Measurement Report Fields

Measurement Tag	Description	Collection Interval
Sbr.TxError	Number of error responses sent during the collection interval	5 min
Sbr.TxShedCreates	Number of load shed error responses per task indicating	5 min

Measurement Tag	Description	Collection Interval
	load shed create sent during the collection interval	
Sbr.TxShedWrites	Number of load shed error responses per task indicating load shed write sent during the collection interval	5 min
Sbr.TxShedReads	Number of load shed error responses per task indicating load shed read sent during the collection interval	5 min
Sbr.TxShedAll	Number of load shed error responses per task indicating load shed all sent during the collection interval	5 min
Sbr.StackQueueFull	Number of StackEvents discarded due to SBR task queue full condition	5 min
Sbr.TxShedCreatesTot	Number of load shed error responses for create operations during the collection interval.	5 min
Sbr.TxShedWritesTot	Number of load shed error responses for write operations during the collection interval.	5 min
Sbr.TxShedReadsTot	Number of load shed error responses for read operations during the collection interval.	5 min
Sbr.TxShedAllTot	Number of load shed error responses for all operations during the collection interval.	5 min

Sbr.TxError

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by return code):

- 0 = Unknown message type
- 1 = SBDB is full
- 2 = SBDB returned an error
- 3 = Session record not found
- 4 = Required parameter was missing
- 5 = Request shed due to load

Description: The number of error responses sent during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application sends an error response.

Measurement Scope: Server Group

Recovery:

1. Any counts for this measurement should be investigated.
2. For counts of unknown message type (return code 0), SBDB errors (return code 2) or missing parameters (return code 4), contact the *Customer Care Center* for assistance.
3. For counts of SBDB is full messages (return code 1), additional capacity may be required. Contact the *Customer Care Center* for assistance.
4. Counts of missing records (return code 3) occur if a session was removed during audit and then another request was received. To prevent this, increase the **Stale SBDB session binding age** setting found on the **CPA** > **Configuration** > **SBR** pane.
5. Any counts of requests shed due to load (return code 5) indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. Also check the Sbr.TxShed measurements to see which requests are being shed.

Sbr.StackQueueFull

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Partition ID)

Description: StackEvents discarded due to the SBR's task queue being full.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR discards a StackEvent due to its task queue being full.

Measurement Scope: Server Group

Measurement Dimension: Arrayed by subresource

Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The *Sbr.TxError* measurement will also show counts when this measurement shows counts.

Sbr.TxShedCreates

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Partition ID)

Description: The number of load shed error responses sent that indicate creation operations shed during the collection interval. Creation operations are shed during minor congestion.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.

Measurement Scope: Server Group

Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The *Sbr.TxError* measurement will also show counts when this measurement shows counts. Another associated measurement, *Sbr.RxIngressMsgQueueAvg*, shows the average percentage of queue length utilization, which is used to determine congestion.

Sbr.TxShedWrites

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Partition ID)

Description: The number of load shed error responses sent that indicate update operations shed during the collection interval. Update operations are shed during major congestion.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.

Measurement Scope: Server Group

Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The *Sbr.TxError* measurement will also show counts when this measurement shows counts. Another associated measurement, *Sbr.RxIngressMsgQueueAvg*, shows the average percentage of queue length utilization, which is used to determine congestion.

Sbr.TxShedReads

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Partition ID)

Description: The number of load shed error responses sent that indicate read operations shed during the collection interval. Read operations are shed during critical congestion.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.

Measurement Scope: Server Group

Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The *Sbr.TxError* measurement will also show counts when this measurement shows counts. Another associated measurement, *Sbr.RxIngressMsgQueueAvg*, shows the average percentage of queue length utilization, which is used to determine congestion.

Sbr.TxShedAll

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Partition ID)

Description: The number of load shed error responses indicating load shed sent during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR transmits a load shed error response.

Measurement Scope: Server Group

Recovery: Any counts for this measurement should be investigated. Counts for this measurement indicate that the SBR may be congested. Inspect the alarms for the SBR for more information regarding the severity of the congestion. The *Sbr.TxError* measurement will also show counts when this measurement shows counts.

Sbr.TxShedCreatesTot

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The system wide number of load shed error responses for create operations during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time the SBR transmits a load shed error response for a create operation.

Measurement Scope: Server Group

Recovery: No action required

Sbr.TxShedWritesTot

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The system wide number of load shed error responses for write operations during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time the SBR transmits a load shed error response for a write operation.

Measurement Scope: Server Group

Recovery: No action required

Sbr.TxShedReadsTot

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The system wide number of load shed error responses for read operations during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time the SBR transmits a load shed error response for a read operation.

Measurement Scope: Server Group

Recovery: No action required

Sbr.TxShedAllTot

Measurement Group: SBR Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: The system wide number of load shed error responses for all operations during the collection interval.

Collection Interval: 5 min

Peg Condition: Each time the SBR transmits a load shed error response for any operation.

Measurement Scope: Server Group

Recovery: No action required

Session Binding Repository (SBR) Performance measurements

The "SBR Performance" measurement group contains measurements that provide performance information that is specific to the SBR application. Counts for various expected/normal messages and events are included in this group. Measurements such as the following are included.

Table 74: SBR Performance Measurement Report Fields

Measurement Tag	Description	Collection Interval
Sbr.RxCreate	Number of create requests received during the collection interval	5 min
Sbr.RxUpdate	Number of update requests received during the collection interval	5 min
Sbr.RxRead	Number of read requests received during the collection interval	5 min
Sbr.RxDelete	Number of delete requests received during the collection interval	5 min
Sbr.RxStatus	Number of status requests received during the collection interval	5 min
Sbr.TxSuccess	Number of success responses sent during the collection interval	5 min
Sbr.RxReqRatePeak	Maximum number of transactions/second processed by the SBR during the reporting interval	5 min
Sbr.RxServTimeAvg	Average transaction service time in microseconds during the reporting interval	5 min
Sbr.RxServTimePeak	Peak transaction service time in microseconds during the reporting interval	5 min
Sbr.EvStaleRecRemoved	Number of stale session binding records cleaned by the audit procedure during the reporting interval	5 min
Sbr.EvCreateUpdateMod	Number of create operations turned into update operations during the reporting interval	5 min
Sbr.EvAvgSessionAge	Average age of all current session bindings	5 min
Sbr.RxReqRateAvg	Average of all message processing rate samples taken during the collection interval	5 min

Measurement Tag	Description	Collection Interval
Sbr.EvSchdStaleRec	Expected number of stale session bindings scheduled for deletion	5 min
Sbr.EvStaleRecRevived	Number of session bindings older than the mostly age that have their timestamps refreshed to the current time	5 min
Sbr.EvMostlyStaleSessPartition	Number of session bindings older than the mostly stale age in each partition	5 min
Sbr.EvAvgSessionAgePartition	Average age of session binding of a partition	5 min
Sbr.RxIngressMsgQueuePeak	Peak SBR Ingress Message Queue utilization measured during the collection interval	5 min
Sbr.RxIngressMsgQueueAvg	Average SBR Ingress Message Queue utilization measured during the collection interval	5 min

Sbr.RxCreate

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of create requests received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application receives a create request.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxUpdate

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of update requests received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application receives an update request.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxRead

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of read requests received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application receives a read request.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxDelete

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of delete requests received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application receives a delete request.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxStatus

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of status requests received during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application receives a status request.

Measurement Scope: Server Group

Recovery: None required

Sbr.TxSuccess

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of success responses sent during the collection interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application sends a success response.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxReqRatePeak

Measurement Group: SBR Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The maximum number of transactions/second processed by the SBR during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement is maximum number of transactions/second processed by the SBR application during the collection interval.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxServTimeAvg

Measurement Group: SBR Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average transaction service time in microseconds during the reporting interval

Collection Interval: 5 min

Peg Condition: This measurement is the average transaction service time in microseconds processed by the SBR application.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxServTimePeak

Measurement Group: SBR Performance

Measurement Type: Max

Measurement Dimension: Single

Description: The peak transaction service time in microseconds during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement is the peak transaction service time in microseconds processed by the SBR application.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvStaleRecRemoved

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of stale session binding records cleaned by the audit procedure during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application removes a stale session binding record during the audit procedure. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvCreateUpdateMod

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of create operations turned into update operations during the reporting interval.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time the SBR application turns a create operation into an update operation. That is, it finds a pre-existing sessionId.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvAvgSessionAge

Measurement Group: SBR Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average age in seconds of all current session bindings.

Collection Interval: 5 min

Peg Condition: This measurement is the average age of all current session bindings processed by the SBR application. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxReqRateAvg

Measurement Group: SBR Performance

Measurement Type: Average

Measurement Dimension: Single

Description: The average message processing rate per second.

Collection Interval: 5 min

Peg Condition: The average of all message processing rate samples per second taken during the collection interval.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvSchdStaleRec

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The expected number of stale session bindings scheduled for deletion.

Collection Interval: 5 min

Peg Condition: This measurement is the expected number of stale session bindings to be deleted during the next stale session binding record audit. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvStaleRecRevived

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: The number of session bindings older than the "mostly age" that have their timestamps refreshed to the current time.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time a session binding that is older than the "mostly stale" age has its timestamp refreshed to the current time.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvMostlyStaleSessPartition

Measurement Group: SBR Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Partition ID)

Description: The number of session bindings older than the "mostly stale" age in each partition.

Collection Interval: 5 min

Peg Condition: This measurement is incremented by one each time a session binding becomes older than the "mostly stale" age. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.

Measurement Scope: Server Group

Recovery: None required

Sbr.EvAvgSessionAgePartition

Measurement Group: SBR Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Partition ID)

Description: The average age in seconds of session binding of a partition.

Collection Interval: 5 min

Peg Condition: This measurement will be computed during each partition's audit process and updated appropriately. This measurement only shows counts in the collection interval that occurs immediately after the audit has run.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxIngressMsgQueuePeak

Measurement Group: SBR Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Partition ID)

Description: The peak SBR Ingress Message Queue utilization measured during the collection interval

Collection Interval: 5 min

Peg Condition: This measurement is the peak ingress message queue utilization by the SBR application.

Measurement Scope: Server Group

Recovery: None required

Sbr.RxIngressMsgQueueAvg

Measurement Group: SBR Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Partition ID)

Description: The average SBR Ingress Message Queue utilization in percent measured during the collection interval. This measurement, if it goes above 85% percent, will trigger a congestion alarm.

Collection Interval: 5 min

Peg Condition: This measurement is the average ingress message queue utilization in percent by the SBR application.

Measurement Scope: Server Group

Recovery: None required

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

Measurement Tag	Description	Collection Interval
TxPathTopology	Number of messages given path topology hiding treatment on messages routed to an Untrusted Network.	5 min
RxPathTopology	Number of messages given path topology hiding treatment on messages received from an Untrusted Network.	5 min
EvHssTopology	Number of messages given S6a/S6d HSS topology hiding treatment.	5 min
EvMmeTopology	Number of messages given MME/SGSN topology hiding treatment.	5 min
EvMmeTopologyException	Number of messages given exception treatment while applying MME/SGSN topology hiding treatment.	5 min
EvHssTopologyException	Number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment.	5 min
TxPathTopologyMp	Number of messages given path topology hiding treatment on messages routed to an Untrusted Network.	5 min
RxPathTopologyMp	Number of messages given path topology hiding treatment on messages received from an Untrusted Network.	5 min
EvHssTopologyMp	Number of messages given S6a/S6d HSS topology hiding treatment.	5 min
EvMmeTopologyMp	Number of messages given MME/SGSN topology hiding treatment.	5 min
EvMmeTopologyMpException	Number of messages given exception treatment while applying MME/SGSN topology hiding treatment.	5 min
EvHssTopologyMpException	Number of messages given exception treatment while applying S6a/S6d HSS topology hiding treatment.	5 min

TxPathTopology

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

No action required

RxPathTopology

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

No action required

EvHssTopology

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

No action required

EvMmeTopology

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

No action required

EvMmeTopologyException

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:

Peg Condition: When MME/SGSN TH exception treatment is applied to either a Request or Answer message at RTH and ATH trigger points.

Recovery:

Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set

EvHssTopologyException

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:

Peg Condition: When S6a/S6d HSS TH exception treatment is applied to Request at RTH trigger point.

Recovery:

Check with the HSS Vendor and request the vendor to be RFC 6733 Compliant.

TxPathTopologyMp

Measurement Group: Topology Hiding Performance

Measurement Type: Simple

Measurement Dimension: Single

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

No action required

RxPathTopologyMp

Measurement Group: Topology Hiding Performance

Measurement Type: Simple

Measurement Dimension: Single

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

No action required

EvHssTopologyMp

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

No action required

EvMmeTopologyMp

Measurement Group: Topology Hiding Performance

Measurement Type: Simple

Measurement Dimension: Single

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

No action required

EvMmeTopologyExceptionMp

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:

Peg Condition: When MME/SGSN TH exception treatment is applied to either a Request or Answer message at RTH and ATH trigger points.

Recovery:

Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set

EvHssTopologyExceptionMp

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:

Peg Condition: When S6a/S6d HSS TH exception treatment is applied to Request at RTH trigger point.

Recovery:

Check with the HSS Vendor and request the vendor to be RFC 6733 Compliant.

Appendix A

Policy DRA Error Resolution Procedures

Topics:

This section provides information and procedures to help users diagnose and resolve internal error codes indexed by the Policy DRA application. These procedures are best used in combination with the *Policy DRA Error Resolution* section of the *Policy DRA User's Guide*.

Error Code 500

Associated Error Category: Missing or Unconfigured APN

Description: Binding capable session initiation request is received with no APN.

Associated P-DRA Alarm/Event: *22730 - Policy DRA Configuration Error*

Associated Measurement: *RxBindCapMissingApn*

Associated Diameter Interface / Message Type: Gx/Gxx CCR-I

GUI Configurable: Yes

Recovery:

1. See *CCR-I Processing with PCRF Pool* and *findOrCreateBinding Response Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where this error occurs and the impacts on Gx/Gxx CCR signaling processing.
2. Go to the P-DRA GUI at **Main Menu** > **Alarms & Events** > **View History**. Set up the right scope for Server Group, Resource Domain, Place and Place Association, or use alarm *22730 - Policy DRA Configuration Error* as Display Filter to start the search.
3. A list of alarm *22730 - Policy DRA Configuration Error* should be displayed. Select an alarm based on the alarm time stamp or other preferred criteria that will bring in the details of the alarm in **Main Menu** > **Alarms & Events** > **View History [Report]**.
4. Obtain the policy client's Origin-Host FQDN from the ERR_INFO in the alarm report on alarm *22730 - Policy DRA Configuration Error*.
5. Go to **Main Menu** > **Measurements** > **Report** to obtain the measurement report for *RxBindCapMissingApn* and other relevant measurements. The frequency of the problem may be observed.
6. If needed, contact the *Customer Care Center* for further assistance.

Error Code 501

Associated Error Category: Missing or Unconfigured APN

Description: Binding capable session initiation request is received with an APN, but the APN is not configured in the APN configuration.

Associated P-DRA Alarm/Event: *22730 - Policy DRA Configuration Error*

Associated Measurement: *RxBindCapUnknownApn*

Associated Diameter Interface / Message Type: Gx/Gxx CCR-I

GUI Configurable: Yes

Recovery:

1. See *CCR-I Processing with PCRF Pool* and *findOrCreateBinding Response Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where this error occurs and the impacts on Gx/Gxx CCR signaling processing.

2. Go to the P-DRA GUI at **Main Menu** > **Alarms & Events** > **View History**. Set up the right scope for Server Group, Resource Domain, Place and Place Association, or use alarm *22730 - Policy DRA Configuration Error* as Display Filter to start the search.
3. A list of alarm *22730 - Policy DRA Configuration Error* should be displayed. Select an alarm based on the alarm time stamp or other preferred criteria that will bring in the details of the alarm in **Main Menu** > **Alarms & Events** > **View History [Report]**.
4. Obtain the policy client's Origin-Host FQDN from the ERR_INFO in the alarm report on alarm *22730 - Policy DRA Configuration Error*.
5. If the APN string is expected, configure the APN at the NOAMP using **Main Menu** > **Policy DRA** > **Configuration** > **Access Point Names** screen.
6. If the APN string is not expected, it may imply that the policy client whose FQDN is specified in the ERR_INFO is using an invalid APN.
7. Go to **Main Menu** > **Measurements** > **Report** to obtain the measurement report for all relevant measurements. The frequency of the problem may be observed.

Error Code 502

Associated Error Category: Binding Found But Unable To Route

Description: Request message is received and a binding with a PRCF was found. Policy DRA can't route the request to PCRF due to DSR queue full error.

Associated P-DRA Alarm/Event: *22707 - Policy DRA Diameter Message Processing Failure*

Associated Measurement: *RxRequestMsgQueueFullDiscard*

Associated Diameter Interface / Message Type:

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. See *findSessionRef Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where this error occurs.
2. Go to the P-DRA NOAM GUI to collect information for possible root causes that may resort in the DRL queue being full:
   - Go to **Main Menu** > **Policy DRA** > **Status & Manage** > **Server** to verify is some DA-MPs have failed. If some servers on the same side fail, the traffic will be distributed amongst the remaining DA-MPs).
   - Go to **Main Menu** > **Status & Manage** > **KPIs** to check the ingress traffic rates of the DA-MPs. Each DA-MP in the site should have about the same ingress rate in normal situation.
   - Go to **Main Menu** > **Alarms & Events** > **View History** to search for relevant congestion alarms. The Display Filter may be set as Timestamp or Server to include P-DRA, DRL, or DCL alarms.
3. Go to **Main Menu** > **Measurements** > **Report** to obtain the measurement report for all relevant measurements.

Error Code 2xx/3xx

Associated Error Category: Binding Found But Unable To Route

Description: Request message is received and a binding with a PRCF was found. Policy DRA can't route the request to PCRF due to PCRF being unreachable.

Associated P-DRA Alarm/Event: *22707 - Policy DRA Diameter Message Processing Failure*

Associated Measurement: *TxPdraAnswersGeneratedForDiameterErr*

Associated Diameter Interface / Message Type:

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. Error code 2xx/3xx is generated by DSR routing layer for various routing errors that result in the failure of routing the Diameter request to the PCRF.
2. Go to the P-DRA NOAM GUI to check the server status from **Main Menu** > **Policy DRA** > **Status & Manage** > **Server** to verify if some DA-MPs have failed (if some servers on the same side fail, the traffic will be distributed amongst the remaining DA-MPs).
3. Go to **Main Menu** > **Status & Manage** > **KPIs** to check the ingress traffic rates of the DA-MPs. Each DA-MP in the site should have about the same ingress rate in normal situation
4. Go to **Main Menu** > **Alarms & Events** > **View History** to search for relevant congestion alarms. The Display Filter may be set as Timestamp or Server to include Policy DRA, DRL, or DCL alarms.
5. Check the Policy DRA SOAM GUI **Main Menu** > **Measurements** > **Report** to search for relevant measurements.

Error Code 510

Associated Error Category: Binding Found But Unable To Route

Description: A slave session could not be routed because, on polling the slave, sessionRef was no longer in the binding database.

Associated P-DRA Alarm/Event: N/A

Associated Measurement: *PsbrSlavePollingFail*

Associated Diameter Interface / Message Type:

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. See *Early binding Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand
2. Go to the P-DRA SOAM GUI at **Main Menu** > **Policy DRA** > **Status & Manage** > **Server** to check binding pSBRs' status.
3. Go to the **Main Menu** > **Alarms & Events** > **View History** to check binding pSBR's congestion alarm/event info to determine a relation with the error.
4. Go to the Policy DRA SOAM GUI **Main Menu** > **Measurements** > **Report** to search for relevant measurements. Select, but not limited to, "pSBR Binding Exception" Measurement Group for the measurements directly related to this error.

Error Code 511

Associated Error Category: Binding Found But Unable To Route

Description: A slave session could not be routed because, on polling the master, sessionRef was no longer in the binding database.

Associated P-DRA Alarm/Event: N/A

Associated Measurement: *PsbrSlavePollingFail*

Associated Diameter Interface / Message Type:

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. See *Early binding Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the P-DRA SOAM GUI at **Main Menu** > **Status & Manage** > **Server** to check binding pSBRs' status.
3. Get the measurement report from **Main Menu** > **Measurements** > **Report** to the frequency of the relevant measurements. Select, but not limited to, "pSBR Binding Exception" Measurement Group to determine the frequency of the relevant measurements.

Error Code 512

Associated Error Category: Binding Found But Unable To Route

Description: A slave session could not be routed because, on polling the master, sessionRef was early too long.

Associated P-DRA Alarm/Event: N/A

Associated Measurement: *PsbrEarlyTooLongSrRemoved*

Associated Diameter Interface / Message Type:

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. Check *Early binding Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the P-DRA SOAM GUI at **Main Menu** > **Status & Manage** > **Server** to obtain the Policy DRA DA-MP and binding pSBR status.
3. Go to the **Main Menu** > **Alarms & Events** > **View History** to obtain the congestion alarm/event for Policy DRA DA-MP and/or binding pSBR, if congestion occurs. Some congestion conditions may be released after a short while. The error may not persist after the congestion condition is gone.
4. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, "pSBR Binding Exception" and "Policy DRA Congestion" Measurement Groups.
5. Go to Policy DRA NOAM GUI at **Main Menu** > **Policy DRA** > **Configuration** > **Network-Wide Options** to check the Maximum Early Binding Lifetime value. Re-configure the value if necessary.

   Note: The measurement *PsbrEarlyTooLongSrRemoved* indicates the frequency at which binding sessionRefs are discovered in an early state for longer than expected. This unexpected condition could occur if the binding pSBR was in congestion and load shedding prevented the session from being transitioned from the early state to a final state. It could also occur if the Maximum Early Binding Lifetime value is configured to be nearly equal to or shorter than the Diameter transaction timer.

Error Code 513

Associated Error Category: Binding Found But Unable To Route

Description: A slave session could not be routed because, on polling the master, an internal error occurred.

Associated P-DRA Alarm/Event: N/A

Associated Measurement: *PsbrSlavePollingFail*

Associated Diameter Interface / Message Type:

- Gx/Gxx CCR-I
- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. Go to the P-DRA SOAM GUI at **Main Menu** > **Status & Manage** > **Server** to obtain the Policy DRA DA-MP and binding pSBR status.
2. Go to the **Main Menu** > **Alarms & Events** > **View History** to obtain the congestion alarm/event for Policy DRA DA-MP and/or binding pSBR, if congestion occurs. Some congestion conditions may be released after a short while. The error may not persist after the congestion condition is gone.
3. Go to Policy DRA SOAM GUI at **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to check the server connection status. The error may be caused by a disconnection between the local and peer nodes that the message was retransmitted the maximum number of times without receiving a response.
4. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, "ComAgent Exception," "Connection Congestion," "pSBR Binding Exception" and "Policy DRA Congestion" Measurement Groups.

Error Code 503

Associated Error Category: No Usable Keys In Binding Dependent Message

Description: No binding key in Binding Key Priority GUI can be matched or no key is included in the binding dependent message.

Associated P-DRA Alarm/Event: *22706 - Binding Key Not Found In Diameter Message*

Associated Measurement: *TxPdraAnswersGeneratedForDiameterErr*

Associated Diameter Interface / Message Type:

- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. Check *AAR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to Policy DRA NOAM GUI at **Main Menu** > **Policy DRA** > **Configuration** > **Binding Key Priority** to verify if the binding key priorities are expected (for instance IMSI and IPv56 Address are expected, but MSISDN and IPv4 are displayed instead).
3. If the binding key priorities are not expected, reset the binding key priority in this screen properly.
4. If the binding key priority are expected, check the validity of the received Request message as follows:
   - AVP carrying the expected key is present in the message
   - AVP carrying the expected key is correctly formed
   - AVP carrying the expected key is using a supported format (e.g. Subscription-ID AVP only Subscription-ID-Type of END_USER_E164 for MSISDN key and END_USER_IMSI for IMSI key).
5. Check the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** to search for all relevant alarms/events. The alarm Display Filter may be set as Timestamp to verify all alarms generated at the same time when the error occurred.

6. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, "pSBR Binding Exception," "pSBR Session Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 505

Associated Error Category: Binding Not Found

Description: Binding record is not found after examining all configured binding keys in Diameter message.

Associated P-DRA Alarm/Event: *22718 - Binding Not Found for Binding Dependent Session Initiate Request*

Associated Measurement: *TxPdraAnswersGeneratedForPsbrErrResp*

Associated Diameter Interface / Message Type:

- Rx AAR
- Gx-Prime CCR-I

GUI Configurable: Yes

Recovery:

1. Check *AAR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to Policy DRA NOAM GUI at **Main Menu** > **Policy DRA** > **Configuration** > **Binding Key Priority** to verify if the binding key priorities are expected (for isntance IMSI and IPv56 Address are expected, but MSISDN and IPv4 are displayed instead).
3. If the binding key priorities are not expected, reset the binding key priority in this screen properly.
4. If the binding key priority are expected, check the validity of the received Request message as follows:
   - AVP carrying the expected key is present in the message
   - AVP carrying the expected key is correctly formed
   - AVP carrying the expected key is using a supported format (e.g. Subscription-ID AVP only Subscription-ID-Type of END_USER_E164 for MSISDN key and END_USER_IMSI for IMSI key).
5. Go to Policy DRA NOAM GUI at **Main Menu** > **Policy DRA** > **Maintenance** > **Binding Key Query** to query the IMSI key to find all alternate keys. If alternate records exist, compare the keys from the database to the keys in the request message to see if they match exactly (e.g. no extra digits or characters, etc.)
6. Check the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** to search for all relevant alarms/events. The alarm Display Filter may be set as Timestamp to verify all alarms generated at the same time when the error occurred.
7. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, "pSBR Binding Exception," "pSBR Session Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 507

Associated Error Category: Policy SBR Error

Description: Policy SBR Error - ComAgent timeout

Associated P-DRA Alarm/Event: *22704 - Policy DRA Communication Agent Error*

Associated Measurement: *TxPdraErrAnsGeneratedCAFailure*

Associated Diameter Interface / Message Type:

- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: Yes

Recovery:

1. Check *findSessionRef Processing*, *findOrCreateBindingResult Processing*, *findOrCreateBinding Response Processing with PCRF Pool*, *findSession Response Processing*, and *AAR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to Policy DRA SOAM GUI at **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to check the server connection status. The error may be caused by a disconnection between the local and peer nodes that the message was retransmitted the maximum number of times without receiving a response. Also check the Communication Agent Service status screen that corresponds to the ServiceID in the event instance to troubleshoot the operation of the service.
3. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, "ComAgent Exception," "Connection Congestion," "pSBR Binding Exception," and "Policy DRA Congestion" Measurement Groups.
4. Check the **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in particular, *19810 - Communication Agent Egress Message Discarded*, *19811 - Communication Agent Ingress Message Discarded*, *19814 - Communication Agent Peer has not responded to heartbeat*, *19832 - Communication Agent Reliable Transaction Failed*, *19833 - Communication Agent Service Egress Message Discarded*, *22712 - Policy SBR Communication Error*, *22722 - Policy DRA Binding Sub-resource Unavailable* , and *22723 - Policy DRA Session Sub-resource Unavailable*.

Error Code 508

Associated Error Category: Policy SBR Error

Description: Policy SBR Error - pSBR database error prevents pSBR from reading, writing, or deleting a record

Associated P-DRA Alarm/Event: *22711 - Policy SBR Database Error*

Associated Measurement: *TxPdraAnswersGeneratedForPsbrErrResp*

Associated Diameter Interface / Message Type:

- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: Yes

Recovery:

1. Check *findSessionRef Processing*, *findOrCreateBindingResult Processing*, *findOrCreateBinding Response Processing with PCRF Pool*, *findSession Response Processing*, and *AAR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to Policy DRA NOAM GUI at **Main Menu** > **Policy DRA** > **Maintenance** > **Policy SBR Status** to verify the status of binding and session pSBR servers.
3. Check the **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in particular, *22711 - Policy SBR Database Error*). The table, operation, and key value of the pSBR DB where the error may occur will be indicated as well.
4. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, "pSBR Binding Exception" and "pSBR Session Exception" Measurement Groups.

Error Code 520

Associated Error Category: Policy SBR Error

Description: Policy SBR PCRF Configuration Error - binding capable session initiation request received, but not PCRFs are configured at the site.

Associated P-DRA Alarm/Event: *22730 - Policy DRA Configuration Error*

Associated Measurement: *TxPdraAnswersGeneratedPcrfConfigErr*

Associated Diameter Interface / Message Type: Gx CCR-I

GUI Configurable: Yes

Recovery:

1. Check *findOrCreateBinding Response Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Check the **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in particular, *22730 - Policy DRA Configuration Error*).
3. If alarm *22730 - Policy DRA Configuration Error* indicates that no PCRF are configured, configure PCRFs at the SOAM GUI at **Main Menu** > **Policy DRA** > **Configuration** > **PCRFs**.

Error Code 521

Associated Error Category: Policy SBR Error

Description: Policy SBR Error - maximum number of Sessions per Binding is Exceeded that fails the binding creation for given IMSI of MSISDN key.

Associated P-DRA Alarm/Event: *22719 - Maximum Number of Sessions per Binding Exceeded*

Associated Measurement: *TxPdraAnswersGeneratedForPsbrErrResp*

Associated Diameter Interface / Message Type: Gx CCR-I, CCR-U, and CCR-T

GUI Configurable: Yes

Recovery:

1. Check *findOrCreateBindingResult Processing* and *findOrCreateBinding Response Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Check the **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in particular, *22719 - Maximum Number of Sessions per Binding Exceeded*).
3. Go to Policy DRA NOAM GUI at **Main Menu** > **Policy DRA** > **Maintenance** > **Binding Key Query** by using event *22719 - Maximum Number of Sessions per Binding Exceeded* to get all the information about session, including session-ids and PCEF FQDNs, to determine if the session is valid.
4. If the sessions exist in the Policy DRA, but not on the PCEF(s), contact the *Customer Care Center* for assistance.

Error Code 504

Associated Error Category: Policy SBR Error

Description: ComAgent resource unavailable when sending stack event to pSBR.

Associated P-DRA Alarm/Event: *22704 - Policy DRA Communication Agent Error*

Associated Measurement: *TxPdraErrAnsGeneratedCAFailure*

Associated Diameter Interface / Message Type:

- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: Yes

Recovery:

1. Check *CCR-I Processing with PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Check the **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in particular, *19810 - Communication Agent Egress Message Discarded*, *19811 - Communication Agent Ingress Message Discarded*, *19814 - Communication Agent Peer has not responded to heartbeat*, *19832 - Communication Agent Reliable Transaction Failed*, *19833 - Communication Agent Service Egress Message Discarded*, and *22712 - Policy SBR Communication Error*.
3. Check the Policy DRA SOAM GUI at **Main Menu** > **Polcy DRA** > **Maintenance** > **Policy SBR Status** to verify the status of the binding pSBR, session pSBR, and related resources/sub-resources (Resource HA Role, Congestion Level, etc.)
4. Go to **Main Menu** > **Communication Agent** > **Maintenance** to verify Connection Status, Routed Services Status, and HA Services Status for resolving ComAgent unavailability.

Error Code 509

Associated Error Category: Session Not Found

Description: Session Not Found - session record doesn't exist for given session ID.

Associated P-DRA Alarm/Event: *22705 - Policy SBR Error Response Received By Policy DRA*

Associated Measurement: *PsbrFindSessDbErr*

Associated Diameter Interface / Message Type:

- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: Yes

Recovery:

1. Check*findSession Response Processing* and *AAR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Check the **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in particular, *22716 - Policy SBR Audit Statistics Report* to find the Session table to see if sessions were removed by audit.
3. Get the measurement report from **Main Menu** > **Measurements** > **Report** for, but not limited to, measurements *PsbrExpiredSessionsFound*, *PsbrCreateSessDbErr*, and *PsbrRemSessRarAttempts*.
4. Check if topology hiding applies to the policy client.

   Note: All checks may help to determine whether the session was never created, or was created, but removed by audit.

Error Code 305

Associated Error Category: Policy DRA Unavailable or Degraded

Description: Policy DRA Unavailable

Associated P-DRA Alarm/Event: *22500 - DSR Application Unavailable*

Associated Measurement: *RxApplUnavailableForRequest*

Associated Diameter Interface / Message Type:

- All Gx requests
- All Rx Requests
- All Gx-Prime Requests

GUI Configurable: Yes

Recovery:

1. Go to the P-DRA SOAM GUI at **Main Menu** > **Diameter** > **Maintenance** > **Applications** to verify Policy DRA's admin state is set as expected.
2. Check the **Main Menu** > **Diameter** > **Maintenance** > **Applications** to verify Policy DRA's Operational Status and Congestion Level. Policy DRA's Operational Status is "Unavailable" when the operator has removed Policy DRA from service (Admin State is "Disabled").
3. Check **Main Menu** > **Alarms & Events** > **View History** for relevant events or alarms related to this DA-MP server.
4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, measurement *RxApplUnavailableForAnswer*.

Error Code 305

Associated Error Category: Policy DRA Unavailable or Degraded

Description: Policy DRA Degraded

Associated P-DRA Alarm/Event: *22501 - DSR Application Degraded*

Associated Measurement: *RxApplUnavailableForRequest*

Associated Diameter Interface / Message Type:

- All Gx requests
- All Rx Requests
- All Gx-Prime Requests

GUI Configurable: Yes

Recovery:

1. Go to the P-DRA SOAM GUI at **Main Menu** > **Diameter** > **Maintenance** > **Applications** to verify Policy DRA's admin state is set as expected.
2. Check the **Main Menu** > **Diameter** > **Maintenance** > **Applications** to verify Policy DRA's Operational Status and Congestion Level. Policy DRA's Operational Status is "Unavailable" when the operator has removed Policy DRA from service (Admin State is "Disabled").
3. Check **Main Menu** > **Alarms & Events** > **View History** for relevant events or alarms related to this DA-MP server.
4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, measurement *RxApplUnavailableForAnswer*.

Error Code 522

Associated Error Category: Session ID is missing from Request

Description: Session ID is missing from Request

Associated P-DRA Alarm/Event: *22700 - Protocol errors in Diameter Requests*

Associated Measurement: *RxPdraRequestProtocolErr*

Associated Diameter Interface / Message Type:

- All Gx requests
- All Rx Requests
- All Gx-Prime Requests

GUI Configurable: No (Result Code 5005)

Recovery:

1. Check *Diameter Message Validation* and *CCR-I Processing without PCRF Pool* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in paritucular, *22700 - Protocol errors in Diameter Requests*).
3. Use the Origin-Host value of the received Request found in *22700 - Protocol errors in Diameter Requests* to understand from where the Request was sent.
4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, "Diameter Exception," "DSR Application Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 523

Associated Error Category: CC-Request-Type AVP is missing from CCR message

Description: CC-Request-Type AVP is missing from CCR message

Associated P-DRA Alarm/Event: *22700 - Protocol errors in Diameter Requests*

Associated Measurement: *RxPdraRequestProtocolErr*

Associated Diameter Interface / Message Type: Gx CCR-I, CCR-U, and CCR-T

GUI Configurable: No (Result Code 5005)

Recovery:

1. Check *CCR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in paritucular, *22700 - Protocol errors in Diameter Requests*).
3. Use the Origin-Host value of the received Request found in *22700 - Protocol errors in Diameter Requests* to understand from where the Request was sent.
4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, "Diameter Exception," "DSR Application Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 525

Associated Error Category: Invalid AVP value in request message

Description: Invalid AVP value in request message

Associated P-DRA Alarm/Event: *22700 - Protocol errors in Diameter Requests*

Associated Measurement: *RxPdraRequestProtocolErr*

Associated Diameter Interface / Message Type:

- All Gx requests
- All Rx Requests
- All Gx-Prime Requests

GUI Configurable: No (Result Code 5004)

Recovery:

1. Check *CCR Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in paritucular, *22700 - Protocol errors in Diameter Requests*).
3. Use the Origin-Host value of the received Request found in *22700 - Protocol errors in Diameter Requests* to understand from where the Request was sent.
4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, "Diameter Exception," "DSR Application Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 506

Associated Error Category: Destination-Host AVP is missing in in-session request

Description: Destination-Host AVP is missing in in-session request

Associated P-DRA Alarm/Event: *22700 - Protocol errors in Diameter Requests*

Associated Measurement: *RxPdraRequestProtocolErr*

Associated Diameter Interface / Message Type:

- Gx CCR-I, CCR-U, and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U, and CCR-T

GUI Configurable: No (Result Code 5012)

Recovery:

1. Check *STR Processing* and *ASR/ASA Processing* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in paritucular, *22700 - Protocol errors in Diameter Requests*).
3. Use the Origin-Host value of the received Request found in *22700 - Protocol errors in Diameter Requests* to understand from where the Request was sent.

4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, "Diameter Exception," "DSR Application Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 530

Associated Error Category: Unsupported Application ID

Description: Application ID unsupported by Policy DRA

Associated P-DRA Alarm/Event: *22700 - Protocol errors in Diameter Requests*

Associated Measurement: *RxPdraRequestProtocolErr*

Associated Diameter Interface / Message Type: Diameter Requests

GUI Configurable: No (Result Code 3007)

Recovery:

1. Check *Diameter Message Validation* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in paritucular, *22700 - Protocol errors in Diameter Requests*).
3. Use the Origin-Host value of the received Request found in *22700 - Protocol errors in Diameter Requests* to understand from where the Request was sent.
4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, "Diameter Exception," "DSR Application Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Error Code 531

Associated Error Category: Command Code and App ID no match

Description: Command Code doesn't match the App ID or doesn't exist

Associated P-DRA Alarm/Event: *22700 - Protocol errors in Diameter Requests*

Associated Measurement: *RxPdraRequestProtocolErr*

Associated Diameter Interface / Message Type: Diameter Requests

GUI Configurable: No (Result Code 5019)

Recovery:

1. Check *Diameter Message Validation* in the Error Resolution appendix of the *Policy DRA User Guide* to investigate and understand the circumstances where the error occurs.
2. Go to the Policy DRA SOAM GUI at **Main Menu** > **Alarms & Events** > **View History** and set the Display Filter by Event-IDs (in paritucular, *22700 - Protocol errors in Diameter Requests*).
3. Use the Origin-Host value of the received Request found in *22700 - Protocol errors in Diameter Requests* to understand from where the Request was sent.

4. Get the measurement report from **Main Menu** > **Measurement** > **Report** for, but not limited to, "Diameter Exception," "DSR Application Exception," and "Policy DRA Diameter Exception" Measurement Groups.

Glossary

A

AAR	Authentication, Authorization Request (Rx Diameter command)
APN	Access Point Name The name identifying a general packet radio service (GPRS) bearer service in a GSM mobile network. See also GSM.
ASR	Abort-Session-Request
ATH	Application Trouble Handler Answer Topology Hiding
ATR	Application-terminated routing Routing rule that operates on outgoing application-terminated (AT) messages. Answer Topology Restoral (DSR)
AVP	Attribute-Value Pair The Diameter protocol consists of a header followed by one or more attribute-value pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.

B

BIOS	Basic Input-Output System

B

	Firmware on the CPU blade that is executed prior to executing an OS.

C

CAPM	Computer-aided policy making
CCA	Credit Control Answer The Diameter message that is received from the prepaid rating engine to acknowledge a CCR command.
CCR	Continuity Check Request Credit Control Request A Diameter message to be sent to a prepaid rating engine to request credit authorization for an SMS.
CCR-I	CCR Initial
CEA	Capability-Exchange-Answer The Diameter response that the prepaid rating engine sends to the Mobile Originated application during capability exchanges.
CER	Capabilities-Exchange-Request A Diameter message that the Mobile Originated application sends to a prepaid rating engine to perform a capability exchange. The CER (indicated by the Command-Code set to 257 and the Command Flags' 'R' bit set) is sent to exchange local capabilities.The prepaid rating engine responds with a Capability-Exchange-Answer (CEA) message.

C

Charging Proxy Application	A DSR Application that is responsible for sending and receiving Diameter accounting messages.
CMOS	Complementary Metal Oxide Semiconductor CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.
ComAgent	Communication Agent A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.
COMCOL	Communications Core Object Library A suite of re-usable C++ libraries, as well as processes and procedures available for use in Tekelec products. Many of its features are focused toward the communications area of software developments, although it purpose is not intended to restrict its functionality to any particular area
Communication Agent	See ComAgent.
CPA	Capability Point Code ANSI Charging Proxy Application

C

	The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.
CSV	Comma-separated values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

DA-MP	Diameter Agent Message Processor A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP. A computer or blade that is hosting a Diameter Signaling Router Application.
DB	Database Daughter Board Documentation Bulletin Data bus
DCL	Diameter Connection Layer The software layer of the Eagle XG Diameter stack which implements Diameter transport connections.
Diameter	Diameter can also be used as a signaling protocol for mobility

D

	management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty. Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment.
DIH	Diameter Intelligence Hub A troubleshooting solution for LTE, IMS, and 3G Diameter traffic processed by the DSR. DIH does not require separate probes or taps.
DNS	Domain Name Services Domain Name System A system for converting Internet host and domain names into IP addresses.
DP	Data Processor The repository of subscriber data on the individual DSR node elements. The DP hosts the full address resolution database.
DPA	Disconnect-Peer-Answer A message used by a Diameter node to answer the Disconnect-Peer-Request (DPR).

D

DPR	Disconnect-Peer-Request A message used by a Diameter node to inform its peer of its intent to disconnect the transport layer. Upon receipt of a DPR, the Disconnect-Peer-Answer (DPA) is returned.
DRL	Diameter Routing Layer The software layer of the Eagle XG Diameter stack that implements Diameter routing.
DSR	Data Set Ready Diameter Signaling Router A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes. Delete Subscriber Data Request
DWA	Device-Watchdog-Answer A Diameter message used with the Device-Watchdog-Request (DWR) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the prepaid rating engine within the configured timeout period, a DWR message is sent to the prepaid rating engine. If the prepaid rating engine fails to respond with a DWA within the required time, the connection is closed with the prepaid rating engine and initiates failover procedures. All new and pending

D

	requests are then sent to the secondary server.
DWR	Device-Watchdog-Request A Diameter message used with the Device-Watchdog-Answer (DWA) message to proactively detect connection failures. If no traffic is detected on a connection between the Mobile Originated application and the Diameter server within the configured timeout period, a DWR message is sent to the Diameter Server. If the Diameter server fails to respond within the required time, the connection is closed with the Diameter server and initiates failover procedures. All new and pending requests are then sent to the secondary Diameter server.

E

EMR	Egress Message Rate
EPT	Egress Pending Transaction. The number of transactions pending for answers on a connection or peer (or a group of connections/peers)
ETG	Egress Throttle Group (s)
ETG-PCL	Egress Throttle Group Pending Transaction Limiting Congestion Level. ETG-PCL of 0 denotes that state of Rate Limiting function is Normal. ETG-PCL of X (X >0) denotes that Requests of Priority less than X will not be allowed to send to Peers or Diameter Connections in that ETG.

E

ETG-RCL	Egress Throttle Group - Rate Limiting Congestion Level. ETG-RCL of 0 denotes that state of Rate Limiting function is Normal . ETG-RCL of X (X > 0) denotes that Requests of Priority less than X will not be allowed to send to Peers or Diameter Connections in that ETG.

F

FABR	Full Address Based Resolution Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.
Full Address Based Resolution	See FABR.

G

GGA	Get-Gateway-Answer A reply to a GGR. It contains session information for the subscriber present in the GGR. GGA includes the bindings for the subscriber such as, Access Point Name, PCEF FQDN and Creation timestamp. The session information is aggregated in the GGA based on the PCRF to which is it assigned.
GGR	Get-Gateway-Request A request for information for either an IMSI or an MSISDN. Only one subscriber (IMSI or MSISDN) is allowed to be queried per GGR. The GGR is generated by the GQC.
GLA	Gateway Location Application A DSR Application that provides a

G

	Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding and session information is populated in the pSBR-B by the Policy Diameter Routing Agent (Policy DRA). GLA provides methods for a Diameter node to query binding information stored in the pSBR-B. The query can be by either IMSI or MSISDN. GLA processes Diameter Requests and generates Diameter Answers.
GQC	Gateway Query Client also known as Diameter Node
GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.
GWS	Gateway Screening Used at gateway STPs to limit access into the network to authorized users. A gateway STP performs inter-network routing and gateway screening functions. GWS controls access to nonhome SS7 networks. Only an MSU that matches predefined criteria in the EAGLE 5's database is allowed to enter the EAGLE 5.
Gx	The Diameter credit control based interface between a PCRF and a PCEF as defined by 3GPP. The interface is used to convey session information from the PCEF to the

G

	PCRF, and in reply the PCRF provides rule information for the PCEF to enforce.
Gx-Prime	A vendor specific Gx like interface with minor variations as the protocol for DPI and PCRF communications before the standardized Sd reference point/protocol was available. Gx-Prime uses the same Application Id (16777238) as Gx does and the same command code set (Credit Control Request/Answer and Re-Auth Request/Answer) as well.

H

HA	High Availability High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.
HP	Hewlett-Packard
HSS	Home Subscriber Server A central database for subscriber information.

I

IDIH	Integrated Diameter Intelligence Hub
IMSI	International Mobile Subscriber Identity A unique internal network ID identifying a mobile subscriber.

I

	International Mobile Station Identity
IMR	Ingress Message Rate
IPFE	IP Front End A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

K

KPI	Key Performance Indicator

M

Message Processor	See MP
MME	Mobility Management Entity
MP	Message Processor The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.
MSISDN	Mobile Station International Subscriber Directory Number The MSISDN is the network specific subscriber number of a mobile communications subscriber.

M

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

N

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

O

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

O

OOS	Out of Service

P

PCRF	Policy and Charging Rules Function. The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.
P-DRA	Policy DRA
PDU	Protocol Data Unit
Peer	A Diameter node to which a given Diameter node has a direct transport connection.
pSBR	Policy SBR
PTR	Pending Transaction Record

R

Range Based Address Resolution	See RBAR.
RAR	Re-Authorization Request (Gx or Rx Diameter command)
RBAR	Range Based Address Resolution

R

	A DSR enhanced routing application which allows the user to route Diameter end-to-end transactions based on Application ID, Command Code, "Routing Entity" Type, and Routing Entity address ranges.
Relay Agent	Diameter agent that forwards requests and responses to other Diameter nodes based on routing-related AVPs (such as Destination-Realm) and routing configuration. Because relays do not make policy decisions, they do not examine or alter non-routing AVPs. As a result, relays never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are capable of handling any Diameter application or message type.
REPL	Replication
RTH	Request Topology Hiding - A Topology Hiding trigger point that identifies a location within Diameter routing where topology-related information in a Request message is hidden or obscured based upon a set of Topology Hiding rules.
RTR	Router Routes all types of SMS traffic. Request Topology Restoral

S

SBR	Subsystem Backup Routing

S

	Session Binding Repository - A highly available, distributed database for storing Diameter session binding data
Session Binding Repository	See SBR.
SGSN	Serving GPRS Support Node
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance Site Operations, Administration, and Maintenance
SOAP	Simple Object Access Protocol
STR	Send_to_Resource AIN message Session Termination Request (Rx Diameter command)
SW	Software Switch

T

T

TH	Topology Hiding
TTR	Team Test Ready Triggerless TCAP Relay

U

Untrusted Network	A Diameter network which has topology information hidden by the Topology Hiding features.