Oracle® Communications Diameter Signaling Router

Subscriber Data Server Alarms, KPIs, and Measurements User's Guide

E57486 Revision 01

April 2013

ORACLE®

Oracle® Communications Subscriber Data Server Alarms, KPIs, and Measurements User's Guide

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

Overview

The *SDS Alarms, KPIs, and Measurements* documentation provides information about SDS alarms and events, 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 SDS feature. The manual provides preventive and corrective procedures that will aid personnel in maintaining the SDS.

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 Tekelec *My Oracle Support (MOS)*, and *Locate Product Documentation on the Oracle Technology Network Site*.
- *User Interface Introduction* describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.
- *Alarms 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.

Documentation Admonishments

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

Table 1: Admonishments

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

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications* document. The *Related Publications* document is published as a part of the *Release Documentation* and is also published as a separate document on the Tekelec Customer Support Site.

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.

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

Customer Training

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

http://education.oracle.com/communication

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

www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

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

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

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

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

Chapter 2

User Interface Introduction

Topics:

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

User interface organization

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

User Interface Elements

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

Table 2: User interface elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.
Session Banner	Next bar across the top of the web page	The left side of the banner just above the Main Menu provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner: • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates that a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • **Page Title Area**: Occupies the top of the work area. It displays the title of the current page being

Element	Location	Function
		displayed, the date and time, and includes a link to context-sensitive help. • **Page Control Area**: Is located below the Page Title Area, and is used to show controls for the Page Area (this area is optional). When available for an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • **Page Area**: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Splash Page Welcome Message*.

Main menu options

The menu options that appear on the screen differ according to whether you are logged into an SDS or DP SOAM. This table describes all main menu user interface options.

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

Menu Item	Function
Administration	The Administration menu allows you to: • Set up and manage user accounts • Configure group permissions • View session information • Authorize IP addresses to access the user interface • Configure options including, but not limited to, password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Configure SNMP services • Validate and transfer ISO files

Menu Item	Function
	• Prepare, initiate, monitor, and complete upgrades • View the software versions report
Configuration	Provides access to configuring network elements, servers, server groups, and systems.
Alarms & Events	Lists active alarms and alarm history.
Security Log	Allows you to view and export security log data.
Status & Manage	Allows you to monitor the statuses of server processes, both collectively and individually, as well as perform actions required for server maintenance. Also allows you to view the status of file management systems, and to manage data files on servers throughout the system.
Measurements	Allows you to view, modify, import, and export measurement data.
Communication Agent	Provides infrastructure features and services for enabling inter-server communication.
SDS	Provides maintenance and configuration options related to SDS.
Help	Launches the online help system for the user interface.
Logout	Allows you to log out of the user interface.

Common Graphical User Interface Widgets

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

System Login Page

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

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

certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request.

Customizing the Login Message

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

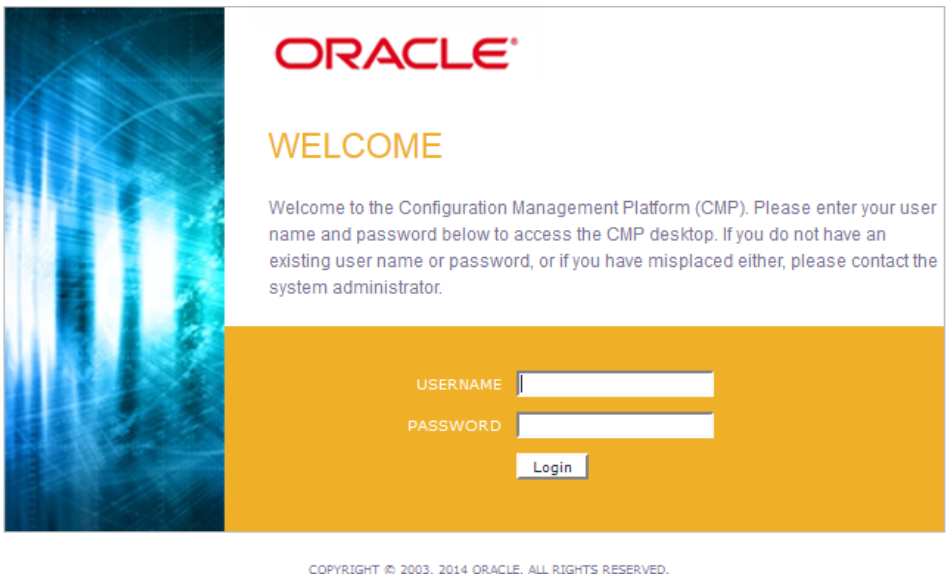


Figure 1: Oracle System Login

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

   The **General Options Administration** page appears.

2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.

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

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

Supported Browsers

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

Main Menu Icons

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

Table 3: Main Menu icons

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

Work Area Displays

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

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

Tables

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

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

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

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

Figure 2: Paginated table

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

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

Export

Figure 3: Scrollable table

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

Forms

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

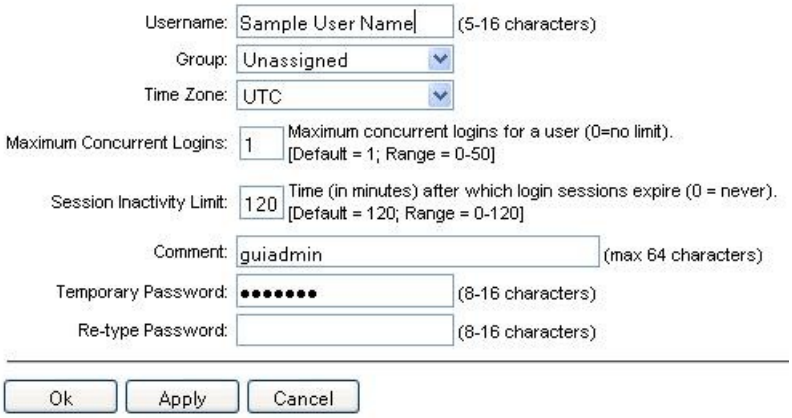


Figure 4: Form page

Tabbed pages

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

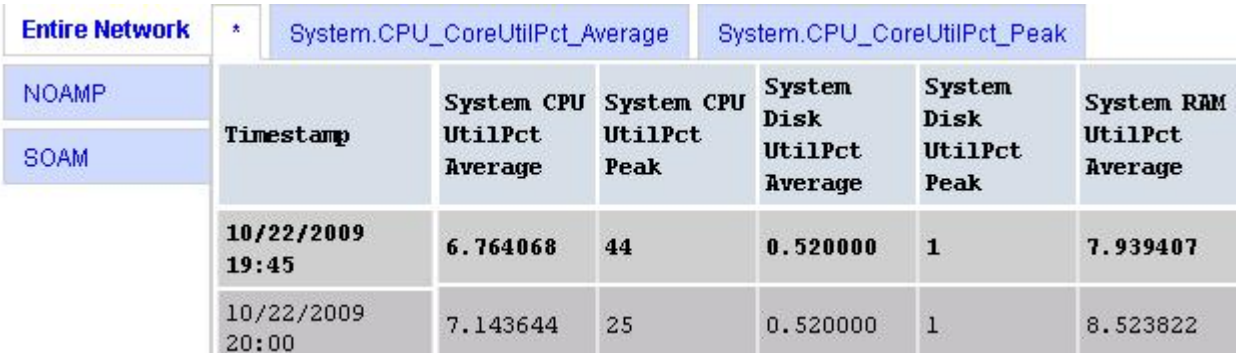


Figure 5: Tabbed pages

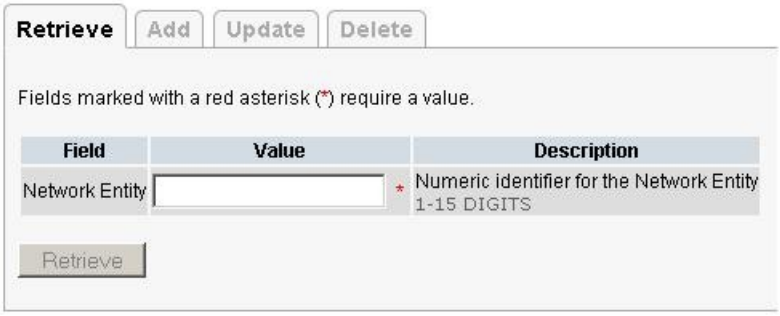


Figure 6: Tabbed pages

Reports

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

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

User Account Usage Report

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

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

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

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

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

End of User Account Usage Report

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

Figure 7: Report output

Customizing the Splash Page Welcome Message

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

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

   The **General Options Administration** page appears.

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

3. Enter the welcome message text in the **Value** column.
4. Click **Update OK** or **Apply** to submit the information.

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

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

Column headers (sorting)

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

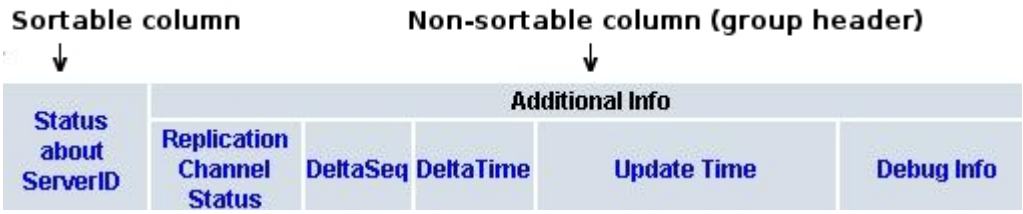


Figure 8: Sortable and Non-sortable Column Headers

Page Controls

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

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

Table 4: Example Action buttons contains examples of Action buttons.

Table 4: Example Action buttons

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

Some Action buttons take you to another page.

Submit buttons, described in *Table 5: Submit buttons*, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information.

The submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 5: Submit buttons

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

Optional Layout Element Toolbar

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

Figure 9: Optional Layout Element Toolbar

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

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

Notifications

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

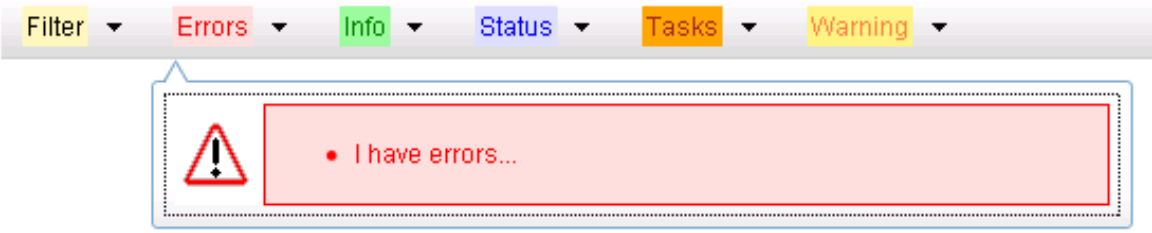


Figure 10: Automatic Error Notification

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

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

Opening an Element in the Toolbar

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

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

Filters

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

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

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

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

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

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

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

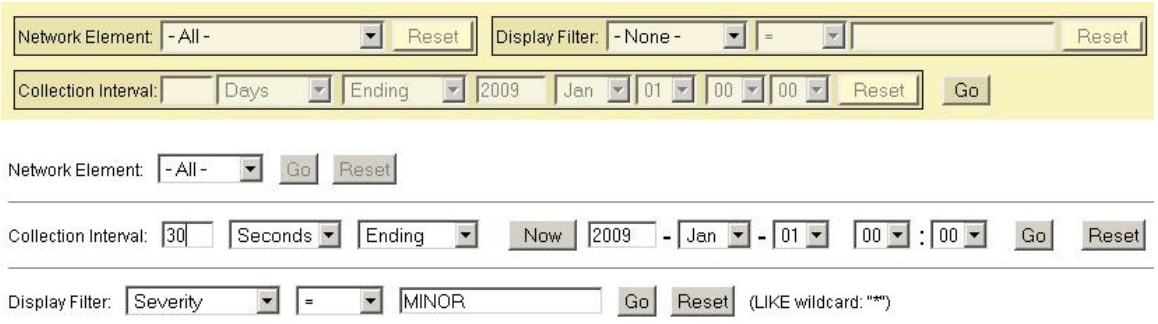


Figure 11: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 6: Filter control elements

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

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

Filtering on the Network Element

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

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

Records are displayed according to the specified criteria.

Filtering on Collection Interval

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

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Enter a duration for the **Collection Interval** filter.
   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.

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

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

Records are displayed according to the specified criteria.

Filtering using the Display Filter

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

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Select a field name from the **Display Filter** pulldown menu.

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

   The selected field name displays in the **Display Filter** field.
3. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.
4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (**=**) operator and a value of MINOR, the table would show only records where Severity=MINOR.
5. For data tables that support compound filtering, click the **Add** button to add another filter condition. Then repeat steps 2 through 4.
   Multiple filter conditions are joined by an AND operator.
6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Auto refresh controls

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

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

Auto Refresh : 15 | **30** | Off

Pause Updates

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

Max Records Per Page Controls

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

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

   The **General Options Administration** page appears.

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

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

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

   OK saves the change and returns to the previous page.

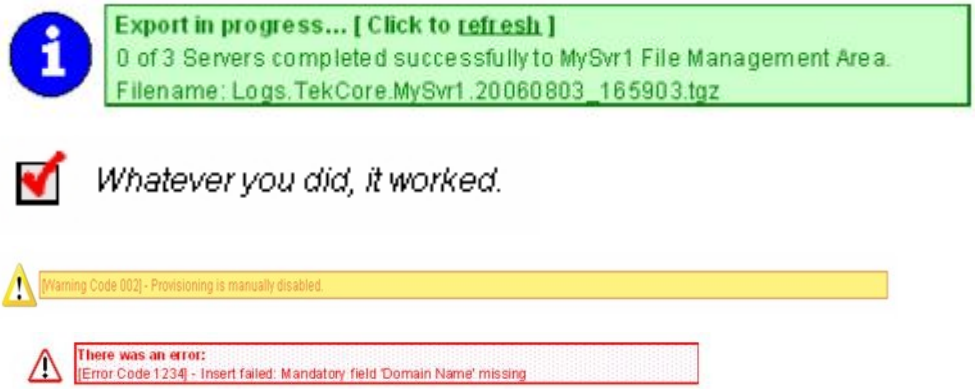
   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Message display

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

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



Chapter 3

Alarms and Events, KPIs, and Measurements Overview

Topics:

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

Alarms Warning

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

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 7: Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server.	Must be a valid hostname, IPv4 address, or IPv6 address. Range: Maximum length is 255 characters; alphanumeric characters (a-z, A-Z, and 0-9) and

Element	Description	Data Input Notes
		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
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

Element	Description	Data Input Notes
		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
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 8: 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 9: 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 10: Scheduled Tasks Elements

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

Editing a scheduled task

Use this procedure to edit a scheduled task.

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

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

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

Deleting a scheduled task

Use this procedure to delete one or more scheduled tasks.

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

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

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

Generating a scheduled task report

Use this procedure to generate a scheduled task report.

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

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

2. Select one or more tasks.

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

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

Chapter 4

Alarms and Events

Topics:

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

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

General alarms and events information

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

Alarms and events overview

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

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

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

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

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

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

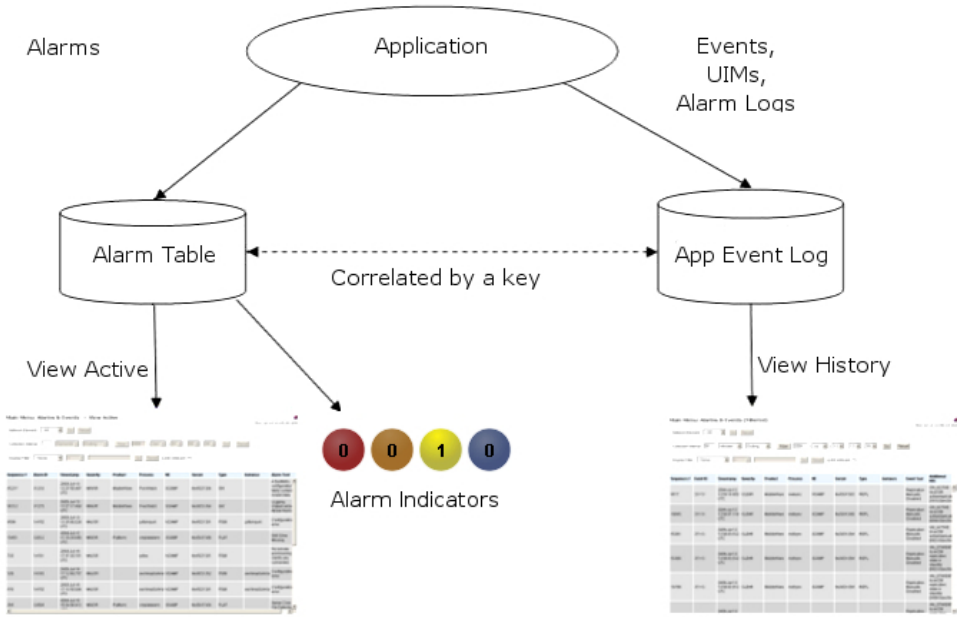


Figure 12: Flow of Alarms

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

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

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

●	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 13: Alarm Indicators Legend

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

Figure 14: Trap Count Indicator Legend

Alarm and event ID ranges

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

Table 11: 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
FABR	22600-22640
PDRA	22700-22799
CPA	22800-22849
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32700
DM-IWF	33000-33024
Load Generator	33025-33049
MD-IWF	33050-33099
GLA	33100-33149

Alarm and event types

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

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

Table 12: 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
DAS	Diameter Application Server (Message Copy)
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
HSS	Home Subscriber Server
IDIH	Integrated DIH
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOADGEN	Load Generator
LOG	Logging
MEAS	Measurements
MEM	Memory
NP	Number Portability
OAM	Operations, Administration & Maintenance

Type Name	Type
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 13: 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 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

Element	Description	Data Input Notes
		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**.

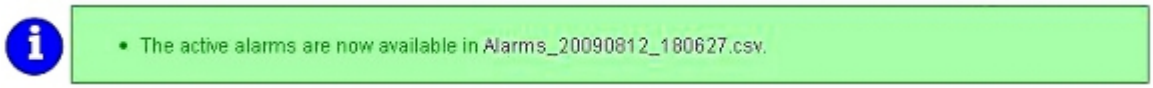
8. Click **OK** or **Apply** to initiate the active alarms export task.

   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 14: 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.
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.

OAM (10000-10999)

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

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

10000 - Incompatible database version

Alarm Group: DB

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

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: 300

OID: tekelecIncompatibleDatabaseVersionNotify

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

10001 - Database backup started

Event Type: DB

Description: The database backup has started.

Severity: Info

Instance: GUI

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupStartNotify

Recovery: No action required.

10002 - Database backup completed

Event Type: DB

Description: Backup completed

Severity: Info

Instance: GUI

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupCompleteNotify

Recovery:

No action required.

10003 - Database backup failed

Event Type: DB

Description: The database backup has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecBackupFailNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10004 - Database restoration started

Event Type: DB

Description: The database restoration has started.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreStartNotify

Recovery:

No action required.

10005 - Database restoration completed

Event Type: DB

Description: The database restoration is completed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreCompleteNotify

Recovery:

No action required.

10006 - Database restoration failed

Event Type: DB

Description: The database restoration has failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: tekelecRestoreFailNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10008 - Database provisioning manually disabled

Alarm Group: DB

Description: Database provisioning has been manually disabled.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecProvisioningManuallyDisabledNotify

Recovery:

No action required.

10009 - Config and Prov db not yet synchronized

Alarm Group: REPL

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

Severity: Critical

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTCfgProvDbNoSyncNotify

Recovery:

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

10010 - Stateful db from mate not yet synchronized

Alarm Group: HA

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

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTStDbNoSyncNotify

Recovery:

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

10011 - Cannot monitor table

Alarm Group: OAM

Description: Monitoring for table cannot be set up.

Severity: Major

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTCantMonitorTableNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10012 - Table change responder failed

Alarm Group: OAM

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

Severity: Major

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTResponderFailedNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10013 - Application restart in progress

Alarm Group: HA

Description: An application restart is in progress.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7OAGTApplSWDisabledNotify

Recovery:

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

10020 - Backup failure

Alarm Group: DB

Description: Database backup failed.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7ApwBackupFailureNotify

Recovery:

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

10050 - Resource Audit Failure

Alarm Group: AUD

Description: Database backup failed.

Severity: Minor

Instance:

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecResourceAuditFailureNotify

Recovery:

10051 - Route Deployment Failed

Alarm Group: AUD

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

Severity: Minor

Instance: Route ID that failed to deploy

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecRouteDeploymentFailedNotify

Recovery:

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

10052 - Route discovery failed

Alarm Group: AUD

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecRouteDiscoveryFailedNotify

Recovery:

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

10053 - Route deployment failed - no available device

Alarm Type: AUD

Description: Could not identify a suitable device for the deployment of a network route

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tekelecNoRouteDevice

Recovery:

1. From AppWorks GUI & CLI, go to **Configuration** > **Network** > **Devices** and verify the devices (network interfaces) for the servers are correct.
2. Contact the *My Oracle Support (MOS)* if the data are verified and the problem still persists.

10054 - Device deployment failed

Alarm Type: AUD

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

Severity: Minor

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tekelecDeviceDeploymentFailed

Recovery:

Collect the logs and contact the *My Oracle Support (MOS)*.

10055 - Device discovery failed

Alarm Group: AUD

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7TekelecDeviceDiscoveryFailedNotify

Recovery:

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

10073 - Server Group Max Allowed HA Role Warning

Alarm Group: HA

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

Severity: Minor

Instance: Affected Server Group name

HA Score: Normal

Auto Clear Seconds: 0

OID: awpss7OAGTSgMaxAllowedHARoleWarnNotify

Recovery:

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

   ```
   # ha.mystate
   ```

10074 - Standby server degraded while mate server stabilizes

Alarm Group: HA

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

Severity: Minor

Instance: N/A

HA Score: Degraded

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7HASbyRecoveryInProgressNotify

Recovery:

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

10075 - Application processes have been manually stopped

Alarm Group: HA

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

Severity: Minor

Instance: N/A

HA Score: Failed

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7HAMtceStopApplicationsNotify

Recovery:

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

Once successfully restarted the alarm will clear.

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

Event Type: HA

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

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7FailureRecoveryWithoutAppRestartNotify

Recovery:

Contact *My Oracle Support (MOS)*.

10100 - Log export started

Event Type: LOG

Description: Log files export operation has started.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportStartNotify

Recovery:

No action required.

10101 - Log export successful

Event Type: LOG

Description: The log files export operation completed successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportSuccessNotify

Recovery:

No action required.

10102 - Log export failed

Event Type: LOG

Description: The log files export operation failed.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportFailedNotify

Recovery:

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

10103 - Log export already in progress

Event Type: LOG

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

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportNotRunNotify

Recovery:

Restart export operation after existing export completes.

10104 - Log export file transfer failed

Event Type: LOG

Description: The performance data export remote copy operation failed.

Severity: Info

Instance: <Task ID>

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

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecExportXferFailedNotify

Recovery:

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

10105 - Log export cancelled - user request

Event Type: LOG

Description: The log files export operation cancelled by user.

Severity: Info

Instance: <Task ID>

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

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportCancelledUserNotify

Recovery:

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

10106 - Log export cancelled - duplicate request

Event Type: LOG

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

Severity: Info

Instance: <Task ID>

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

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportCancelledDuplicateNotify

Recovery:

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

10107 - Log export cancelled - queue full

Event Type: LOG

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

Severity: Info

Instance: <Task ID>

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

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogExportCancelledQueueNotify

Recovery:

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

10108 - Duplicate scheduled log export task

Alarm Group: LOG

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

Severity: Minor

Instance: <Target ID>

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

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecLogExportDupSchedTaskNotify

Recovery:

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

10109 - Log export queue is full

Alarm Group: LOG

Description: The log export queue is full

Severity: Minor

Instance: <Queue Name>

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

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecLogExportQueueFullNotify

Recovery:

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

10151 - Login successful

Event Type: LOG

Description: The login operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLoginSuccessNotify

Recovery:

No action required.

10152 - Login failed

Event Type: LOG

Description: The login operation failed

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLoginFailedNotify

Recovery:

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

10153 - Logout successful

Event Type: LOG

Description: The logout operation was successful.

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 1

OID: awpss7TekelecLogoutSuccessNotify

Recovery:

No action required.

10154 - User Account Disabled

Alarm Group: AUTH

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7TekelecAccountDisabledNotify

Recovery:

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

10155 - SAML Login Successful

Alarm Group: LOG

Description: SAML Login Successful

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: awpss7TekelecSamlLoginSuccessNotify

Recovery:

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

10156 - SAML Login Failed

Alarm Group: LOG

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

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: awpss7TekelecSamlLoginFailedNotify

Recovery:

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

10200 - Remote database reinitialization in progress

Alarm Group: CFG

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

Severity: Minor

Instance: <hostname of remote server>

HA Score: Normal

Auto Clear Seconds: This alarm does not autoclear.

OID: awpss7ApwSgDbReinitNotify

Recovery:

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

SDS (14000-14999)

This section provides information and recovery procedures for SDS alarms and events, ranging from 14000-14999.

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 *General alarms and events information*.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm (Critical, Major, Minor, Informational)
- Instance: where the alarm occurred, for example, GUI, <process name>, IP address, <server name>

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

- HA Score: high availability score; determines if switchover is necessary

- Auto Clear Seconds: the number of seconds that must pass before the alarm will clear itself. Some alarms are not autocleared. Informational events are marked N/A because they do not have to be cleared.
- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

14100 - Interface Disabled

Alarm Type: PROV

Description: Provisioning interface is manually disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not automatically clear after a set time.

OID: sdsProvInterfaceDisabled

Recovery: Enable the interface to clear the alarm.

14101 - No Remote Connections

Alarm Type: PROV

Description: No remote provisioning clients are connected.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: This alarm does not automatically clear.

OID: sdsProvNoRemoteConnections

Recovery: The alarm will clear when at least one remote provisioning client is connected.

14102 - Connection Failed

Alarm Type: PROV

Description: Provisioning client connection initialization failed due to an error specified in additional information. See trace log for details. (CID=<Connection ID>, IP=<IP Address>).

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 300

OID: sdsProvConnectionFailed

Recovery: Alarm automatically clears after 5 minutes or when connected.

14103 - Both Port Identical

Alarm Type: PROV

Description: Both XML and SOAP provisioning client connection are disables since same port is configured for both.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvBothPortIdentical

Recovery: Alarm clears when one of the ports is changed.

14120 - Connection Established

Alarm Type: PROV

Description: Provisioning client connection established.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvConnectionEstablished

Recovery: No action required for this event.

14121 - Connection Terminated

Alarm Type: PROV

Description: Provisioning client connection terminated due to the error specified in additional information.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvConnectionTerminated

Recovery: No action required for this event.

14122 - Connection Denied

Alarm Type: PROV

Description: Provisioning client connection denied due to the error specified in additional information.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvConnectionDenied

Recovery: No action required for this event.

14140 - Import Throttled

Alarm Type: PROV

Description: Provisioning import throttled to prevent overrunning database service processes.

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 5

OID: sdsProvImportThrottled

Recovery: Alarm automatically cleared in 5 seconds after throttling subsides.

14150 - Import Initialization Failed

Alarm Type: PROV

Description: Provisioning import failed due to the initialization error specified in additional information. See trace log for details.

Severity: Major

Instance: provimport

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvImportInitializationFailed

Recovery: Alarm clears when initialization completes successfully.

14151 - Import Generation Failed

Alarm Type: PROV

Description: Provisioning import failed due to the import file execution error specified in the additional information. See the trace log for details.

Severity: Major

Instance: provimport

HA Score: Normal

Auto Clear Seconds: 12 hours

OID: sdsProvImportGenerationFailed

Recovery: Alarm clears automatically after 12 hours or when initialization completes successfully.

14152 - Import Transfer Failed

Alarm Type: PROV

Description: Provisioning import operation failed due to the file transfer error specified in additional information. See trace log for details.

Severity: Major

Instance: provimport

HA Score: Normal

Auto Clear Seconds: 12 hours

OID: sdsProvImportTransferFailed

Recovery: Alarm clears automatically after 12 hours or when the file transfer completes successfully.

14153 - Export Initialization Failed

Alarm Type: PROV

Description: Provisioning export failed due to the initialization error specified in the additional information. See trace log for details.

Severity: Major

Instance: provexport

HA Score: Normal

Auto Clear Seconds: 12 hours

OID: sdsProvExportInitializationFailed

Recovery: Alarm clears automatically after 12 hours or when initialization completes successfully.

14154 - Export Generation Failed

Alarm Type: PROV

Description: Provisioning export operation failed due to the export file generation error specified in the additional information. See trace log for details.

Severity: Major

Instance: provexport

HA Score: Normal

Auto Clear Seconds: 12 hours

OID: sdsProvExportGenerationFailed

Recovery: Correct the problem and try the export again.

14155 - Export Transfer Failed

Alarm Type: PROV

Description: Provisioning export operation failed due to the file transfer error specified in the additional information. See trace log for details.

Severity: Major

Instance: provexport

HA Score: Normal

Auto Clear Seconds: 12 hours

OID: sdsProvExportTransferFailed

Recovery: Correct the problem and try the export again.

14160 - Import Operation Completed

Alarm Type: PROV

Description: All files were imported successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvImportOperationCompleted

Recovery: No action required for this event.

14161 - Export Operation Completed

Alarm Type: PROV

Description: All scheduled exports completed successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvExportOperationCompleted

Recovery: No action required for this event.

14170 - Remote Audit started and in progress

Alarm Type: PROV

Description: Remote Audit started and is in progress.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvRemoteAuditStartedAndInProgressNotify

Recovery: No action required for this event.

14171 - Remote Audit aborted

Alarm Type: PROV

Description: Remote Audit aborted.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvRemoteAuditAbortedNotify

Recovery: No action required for this event.

14172 - Remote Audit failed to complete

Alarm Type: PROV

Description: Remote Audit failed to complete.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvRemoteAuditFailedToCompleteNotify

Recovery: No action required for this event.

14173 - Remote Audit completed

Alarm Type: PROV

Description: Remote Audit completed successfully.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvRemoteAuditCompletedNotify

Recovery: No action required for this event.

14174 - NPA Split pending request deleted

Alarm Type: PROV

Description: A Pending NPA Split has been deleted by the user before it could become Active on its Start Date.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvNpaSplitPendingRequestDeleted

Recovery: No action required for this event.

14175 - NPA Split activation failed

Alarm Type: PROV

Description: NPA Split activation failed. See trace log for details.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvNpaSplitActivationFailed

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

14176 - NPA Split started and is active

Alarm Type: PROV

Description: NPA Split started and is active.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvNpaSplitActivated

Recovery: No action required for this event.

14177 - NPA Split completion failed

Alarm Type: PROV

Description: NPA Split completion failed. See trace log for details.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvNpaSplitCompletionFailed

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

14178 - NPA Split completed

Alarm Type: PROV

Description: NPA Split completed.

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsProvNpaSplitCompleted

Recovery: No action required for this event.

14179 - MSISDN deleted from Blacklist

Alarm Type: PROV

Description: Previously Blacklisted MSISDN is now a Routing Entity

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: sdsProvMsisdnDeletedFromBlacklist

Recovery: No action necessary.

14180 - IMSI deleted from Blacklist

Alarm Type: PROV

Description: Previously Blacklisted IMSI is now a Routing Entity

Severity: Info

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0

OID: sdsProvImsiDeletedFromBlacklist

Recovery: No action necessary.

14188 - PdbRelay not connected

Alarm Type: PROV

Description: PdbRelay not connected.

- The SDS Command Log does not go back far enough to resume relaying commands. A bulk load of HLRR is required.
- Neither Primary nor Disaster Recovery Virtual IP address is configured for the HLRR.
- The connection is failing with the error shown in Additional Info.

Severity: Major

Instance: pdbrelay

HA Score: Normal

Auto Clear Seconds: 0

OID: sdsProvRelayNotConnectedNotify

Recovery:

1. Perform Bulk Load Procedure at the HLRR.
2. Configure the HLRR address in the SDS GUI.
3. Verify network connectivity with the HLRR.

14189 - PdbRelay Time Lag

Alarm Type: PROV

Description: Pdbrelay feature is enabled but is falling behind. The time between timestamps of the last record processed and the latest entry in the Command Log has exceeded time limit threshold.

- Critical: 27 minutes
- Major - 12 minutes
- Minor - 3 minutes

Severity: Critical, Major, Minor

Instance: pdbrelay

HA Score: Normal

Auto Clear Seconds: 0

OID: sdsProvRelayTimeLagNotify

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

14200 - DP Stack Event Queue utilization

Alarm Type: DPS

Description: The percent utilization of the DP Stack Event Queue is approaching its maximum capacity.

Severity:

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

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsDpsStackEventQueueUtilizationNotify

Recovery:

- Minor alarm clears when utilization falls below 50%.
- Major alarm clears when utilization falls below 70%.
- Critical alarm clears when utilization falls below 90%.

14301- ERA Responder Failed

Alarm Type: ERA

Description: Event responder failed due to an internal error.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: sdsEraResponderFailed

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

Communication Agent, ComAgent (19800-19899)

This section provides information and recovery procedures for Communication Agent (ComAgent) alarms and events, ranging from 19800 - 19899, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

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

19800 - Communication Agent Connection Down

Alarm Group: CAF

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnectionDownNotify

Recovery:

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

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

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

19801 - Communication Agent Connection Locally Blocked

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnLocalBlockedNotify

Recovery:

This alarm is cleared when:

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

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

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

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

19802 - Communication Agent Connection Remotely Blocked

Alarm Group: CAF

Description: This alarm indicates that one or more Communication Agent connections have been administratively blocked at a remote server connected to the server, and this is generally done as part

of a maintenance procedure. A connection that is blocked cannot be used by applications to communicate with other servers, and so this alarm may indicate that applications are unable to communicate with their expected set of peers.

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnRemoteBlockedNotify

Recovery:

This alarm is cleared when:

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

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

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

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

19803 - Communication Agent stack event queue utilization

Alarm Group: CAF

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

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFQueueUtilNotify

Recovery:

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

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

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

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

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

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

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

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

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

Alarm Group: CAF

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

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

Severity: Minor

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 300 (5 min)

OID: cAFClientConnWaitNotify

Recovery:

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

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

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

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

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. Verify that the remote server is not under maintenance.
5. If the connection is manually disabled at the client MP, and it is expected to be disabled, then no further action is necessary.
6. If the connection has been manually disabled at the client MP, but it is not supposed to be disabled, then enable the connection by clicking on the 'Enable' action button on the Connection Status screen.
7. Verify that IP network connectivity exists between the two connection end-points.
8. Verify that the connection's local IP address and port number are configured on remote client MP.
9. Verify that the Application Process using Communication Agent plug-in is running on both ends.
10. Verify that the connection's remote IP address and port correctly identify remote's listening port.
11. Contact *My Oracle Support (MOS)* for assistance.

19805 - Communication Agent Failed To Align Connection

Alarm Group: CAF

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnAlignFailedNotify

Recovery:

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

2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
4. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
5. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.

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

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

19806 - Communication Agent CommMessage mempool utilization

Alarm Group: CAF

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

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

Severity: Critical, Major, Minor

Instance: <ComAgent Process Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFPoolResUtilNotify

Recovery:

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

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

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

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

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

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

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

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

19807 - Communication Agent User Data FIFO Queue utilization

Alarm Group: CAF

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

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFUserDataFIFOUtilNotify

Recovery:

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

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

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

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

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

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

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

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

19808 - Communication Agent Connection FIFO Queue utilization

Alarm Group: CAF

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

Severity: Minor, Major, Critical

Instance: <ComAgent StackTask Name>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFMxFIFOUtilNotify

Recovery:

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

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

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

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

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

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

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

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

19810 - Communication Agent Egress Message Discarded

Event Type: CAF

Description: Communication Agent Egress Message Discarded.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventEgressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

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

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

3. If the event is raised due to software condition, It's an indication that the Communication Agent Process may be experiencing problems.
4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
5. Contact *My Oracle Support (MOS)* for assistance.

19811 - Communication Agent Ingress Message Discarded

Event Type: CAF

Description: Communication Agent Ingress Message Discarded.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventIngressMessageDiscardedNotify

Recovery:

1. View the Event AddlInfo column.

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

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

19814 - Communication Agent Peer has not responded to heartbeat

Event Type: CAF

Description: Communication Agent Peer has not responded to heartbeat.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventHeartbeatMissedNotify

Recovery:

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

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

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

19816 - Communication Agent Connection State Changed

Event Type: CAF

Description: Communication Agent Connection State Changed.

Severity: Info

Instance: < RemoteIp >

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventConnectionStateChangeNotify

Recovery:

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

   This Event is a log of connection state change.

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

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

Event Type: CAF

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

Severity: Info

Instance: N/A

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtConfigParamChangeNotify

Recovery:

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

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

3. If the event shows up in **Main Menu** > **Alarms & Events**, without the corresponding GUI security-log in **Main Menu** > **Security Log**. Contact *My Oracle Support (MOS)* for assistance.

19820 - Communication Agent Routed Service Unavailable

Alarm Group: CAF

Description: This alarm indicates that all connections of all connection groups associated with a Routed Service are unavailable. This generally occurs when far-end servers have been removed from service by maintenance actions. This can also occur if all of the Routed Service's connections have been either disabled or blocked.

Severity: Major

Instance: <RoutedServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSUnavailNotify

Recovery:

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

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

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

19821 - Communication Agent Routed Service Degraded

Alarm Group: CAF

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

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSDegradedNotify

Recovery:

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

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

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

19822 - Communication Agent Routed Service Congested

Alarm Group: CAF

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

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSCongestedNotify

Recovery:

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

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

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

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

Alarm Group: CAF

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

Severity: Major

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFRSUsingLowPriConnGrpNotify

Recovery:

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

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

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

19824 - Communication Agent Pending Transaction Utilization

Alarm Group: CAF

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

Severity: Minor, Major, Critical

Instance: n/a (ComAgent process)

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTransUtilNotify

Recovery:

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

   The system may be experiencing network problems.

   The Communication Agent Process may be experiencing problems.

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

19825 - Communication Agent Transaction Failure Rate

Alarm Group: CAF

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

Severity: Minor, Major, Critical

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTransFailRateNotify

Recovery:

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

   The system may be experiencing network problems.

   The Communication Agent Process may be experiencing problems.

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

19826 - Communication Agent Connection Congested

Alarm Group: CAF

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

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFConnCongestedNotify

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
3. Check **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine which connections on the server have abnormal status.
4. If the Remote MP Overload Level (OL) > 0 then determine why the remote server is congested.

a) Verify that the remote server is not under maintenance.
b) Examine the remote's CPU utilization.
c) Examine the remote's current alarms.

5. If the local server's Transport Congestion Level (TCL) > 0 then determine why the connection is not handling the load.
   a) The remote may be overload by traffic from other MPs.
   b) The local server may be trying to send too much traffic to the remote.
   c) The IP connectivity may be impaired.
6. Contact *My Oracle Support (MOS)* for assistance.

19830 - Communication Agent Service Registration State Change

Event Type: CAF

Description: Communication Agent Service Registration State Change.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtSvcRegChangedNotify

Recovery:

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

19831 - Communication Agent Service Operational State Changed

Event Type: CAF

Description: Communication Agent Service Operational State Changed.

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventComAgtSvcOpStateChangedNotify

Recovery:

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

   A service can also change state due to server overload.
2. If the state change is unexpected, then Contact *My Oracle Support (MOS)* for assistance.

19832 - Communication Agent Reliable Transaction Failed

Event Type: CAF

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

Severity: Info

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

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

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventComAgtTransFailedNotify

Recovery:

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

19833 - Communication Agent Service Egress Message Discarded

Event Type: CAF

Description: Communication Agent Service Egress Message Discarded.

Severity: Info

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

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

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventRoutingFailedNotify

Recovery:

1. View the Event AddlInfo column.

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

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

3. If the event is raised due to software condition, It's an indication that the Communication Agent Process may be experiencing problems.
4. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
5. Contact *My Oracle Support (MOS)* for assistance.

19842 - Communication Agent Resource-Provider Registered

Event Type: CAF

Description: Communication Agent Resource-Provider Registered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceProviderRegisteredNotify

Recovery:

No action required.

19843 - Communication Agent Resource-Provider Resource State Changed

Event Type: CAF

Description: Communication Agent Resource-Provider Resource State Changed.

Severity: Info

Instance: <ProviderServerName>: <ResourceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventResourceStateChangeNotify

Recovery:

No action required.

19844 - Communication Agent Resource-Provider Stale Status Received

Event Type: CAF

Description: Communication Agent Resource-Provider Stale Status Received.

Severity: Info

Instance: <ProviderServerName>: <ResourceName>

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventStaleHBPacketNotify

Recovery:

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

19845 - Communication Agent Resource-Provider Deregistered

Event Type: CAF

Description: Communication Agent Resource-Provider Deregistered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceProviderDeRegisteredNotify

Recovery:

No action required.

19846 - Communication Agent Resource Degraded

Alarm Group: CAF

Description: Communication Agent Resource Degraded. A local application is using the resource, identified in the alarm, and the access to the resource is impaired. Some of the resource providers are either unavailable and/or congested.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFResourceCongestedNotify

Recovery:

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

19847 - Communication Agent Resource Unavailable

Alarm Group: CAF

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

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFResourceUnavailNotify

Recovery: Check the Communication Agent Connection Status maintenance screen

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

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

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

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

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

19848 - Communication Agent Resource Error

Alarm Group: CAF

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

Severity: Minor

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 50

OID: cAFResourceErrorNotify

Recovery:

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

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

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

19850 - Communication Agent Resource-User Registered

Event Type: CAF

Description: Communication Agent Resource-User Registered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceUserRegisteredNotify

Recovery:

No action required.

19851 - Communication Agent Resource-User Deregistered

Event Type: CAF

Description: Communication Agent Resource-User Deregistered.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventResourceUserDeRegisteredNotify

Recovery:

No action required.

19852 - Communication Agent Resource Routing State Changed

Event Type: CAF

Description: Communication Agent Resource Routing State Changed.

Severity: Info

Instance: <ResourceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventResourceRoutingStateNotify

Recovery:

No action required.

19853 - Communication Agent Resource Egress Message Discarded

Event Type: CAF

Description: Communication Agent Resource Egress Message Discarded.

Severity: Info

Instance: <ResourceName>: <SubResourceID>

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

HA Score: Normal

Throttle Seconds: 10

OID: cAFEventHaEgressMessageDiscardedNotify

Recovery:

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

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

2. Use **Main Menu** > **Alarms & Events** and examine the alarm log for ComAgent Process problems.
3. Contact *My Oracle Support (MOS)* for assistance.

19854 - Communication Agent Resource-Provider Tracking Table Audit Results

Event Type: CAF

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

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventHaRPTTAuditResultNotify

Recovery:

No action required.

19855 - Communication Agent Resource Has Multiple Actives

Alarm Group: CAF

Description: This alarm indicates a possible IP network disruption that has caused more than one Resource Provider to become Active. The server that asserted this alarm expects there to be only one

active Resource Provider server for the Resource, but instead it is seeing more than one. During this condition the server may be sending commands to the wrong Resource Provider. This may affect applications such as CPA, PDRA.

Severity: Major

Instance: <ResourceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFMultipleActivesNotify

Recovery:

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

19856 - Communication Agent Service Provider Registration State Changed

Event Type: CAF

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

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventSvcProvRegStateChangedNotify

Recovery:

1. This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.
2. Contact *My Oracle Support (MOS)* for further assistance.

19857 - Communication Agent Service Provider Operational State Changed

Event Type: CAF

Description: The Communication Agent Service Provider Operational State has Changed

Severity: Info

Instance: <ServiceName>

HA Score: Normal

Throttle Seconds: 1

OID: cAFEventSvcProvOpStateChangedNotify

Recovery:

1. This event indicates that a ComAgent service provider changed operational state, and typically results from maintenance actions. A service can also change state due to overload.
2. If the state change is unexpected, contact *My Oracle Support (MOS)*.

19860 - Communication Agent Configuration Daemon Table Monitoring Failure

Alarm Group: CAF

Description: This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFTableMonitorFailureNotify

Recovery:

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

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

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

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

5. After NOAM failover completes, verify that the alarm has cleared.
6. If the alarm has not cleared, then Contact *My Oracle Support (MOS)* for assistance.

19861 - Communication Agent Configuration Daemon Script Failure

Alarm Group: CAF

Description: This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity: Critical

Instance: None

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFScriptFailureNotify

Recovery:

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

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

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

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

5. After NOAM failover completes, verify that the alarm has cleared.
6. If the alarm has not cleared, then Contact *My Oracle Support (MOS)* for assistance.

19862 - Communication Agent Ingress Stack Event Rate

Alarm Group: CAF

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

Severity:

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

Instance: <ServiceName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: cAFIngressRateNotify

Recovery:

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

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group: CAF

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

Severity: Info

Instance: <Connection group name>

HA Score: Normal

Throttle Seconds: 86400

OID: cAFComAgentMaxConnsInConnGrpNotify

Recovery:

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

19864 - ComAgent Successfully Set Host Server Hardware Profile

Event Group: CAF

Description: ComAgent successfully set the host server hardware profile.

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventSuccessSetHostServerHWProfileNotify

Recovery:

1. This event indicates that all TPS controlling parameter values are successfully set for the host server hardware profile.
2. If needed, contact *My Oracle Support (MOS)*.

19865 - ComAgent Failed to Set Host Server Hardware Profile

Event Group: CAF

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

Severity: Info

Instance: None

HA Score: Normal

Throttle Seconds: 0 (zero)

OID: cAFEventFailToSetHostServerHWProfileNotify

Recovery:

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

EXG Stack (19000-19999)

This section provides information and recovery procedures for EXG Stack alarms, ranging from 19000-19999.

19900 - DP Server CPU utilization

Alarm Type: STK

Description: The percent utilization of the DP Server CPU is approaching its maximum capacity.

Severity:

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

Instance: N/A

HA Score: Normal

Auto Clear Seconds: N/A

OID: dbcProcessCpuUtilizationNotify

Recovery:

- Minor alarm clears when utilization falls below 57%.
- Major alarm clears when utilization falls below 63%.
- Critical alarm clears when utilization falls below 69%.

19901 - CFG-DB Validation Error

Alarm Group: STK

Description: A minor database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbValidationErrorNotify

Recovery:

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

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

19902 - CFG-DB Update Failure

Alarm Group: STK

Description: A critical database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are DISABLED.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbUpdateFailureNotify

Recovery:

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

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

19903 - CFG-DB post-update Error

Alarm Group: STK

Description: A minor database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity: Major

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbPostUpdateErrorNotify

Recovery:

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

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

19904 - CFG-DB post-update Failure

Alarm Group: STK

Description: A critical database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are DISABLED.

Severity: Critical

Instance: N/A

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcCfgDbPostFailureNotify

Recovery:

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

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

19905 - Measurement Initialization Failure

Alarm Group: STK

Description: A measurement object failed to initialize.

Severity: Critical

Instance: <measTagName>

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: dbcMeasurementInitializationFailureNotify

Recovery:

Measurement subsystem initialization has failed for the specified measurement.

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

19910 - Message Discarded at Test Connection

Event Type: DIAG

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

Severity: Major

Instance: <Connection name>

HA Score: Normal

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.

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 Group: SW

Description: Program impaired by s/w fault

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSwFaultNotify

Recovery:

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

31001 - S/W status

Alarm Group: SW

Description: Program status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSwStatusNotify

Recovery:

No action required.

31002 - Process watchdog failure

Alarm Group: SW

Description: Process watchdog timed out

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolProcWatchdogFailureNotify

Recovery:

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

31003 - Tab thread watchdog failure

Alarm Group: SW

Description: Tab thread watchdog timed out

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolThreadWatchdogFailureNotify

Recovery:

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

31100 - Database replication fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact *My Oracle Support (MOS)*.

31101 - Database replication to slave failure

Alarm Group: REPL

Description: Database replication to a slave Database has failed

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepToSlaveFailureNotify

Recovery:

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

31102 - Database replication from master failure

Alarm Group: REPL

Description: Database replication from a master Database has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepFromMasterFailureNotify

Recovery:

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

31103 - DB Replication update fault

Alarm Group: REPL

Description: Database replication process cannot apply update to DB

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepUpdateFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. Contact *My Oracle Support (MOS)*.

31104 - DB Replication latency over threshold

Alarm Group: REPL

Description: Database replication latency has exceeded thresholds

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepLatencyNotify

Recovery:

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

31105 - Database merge fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeFaultNotify

Recovery:

1. Export event history for the given server and inetmerge task.
2. Contact *My Oracle Support (MOS)*.

31106 - Database merge to parent failure

Alarm Group: COLL

Description: Database merging to the parent Merge Node has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolDbMergeToParentFailureNotify

Recovery:

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

31107 - Database merge from child failure

Alarm Group: COLL

Description: Database merging from a child Source Node has failed

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeFromChildFailureNotify

Recovery:

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

31108 - Database merge latency over threshold

Alarm Group: COLL

Description: Database Merge latency has exceeded thresholds

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeLatencyNotify

Recovery:

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

31109 - Topology config error

Alarm Group: DB

Description: Topology is configured incorrectly

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolTopErrorNotify

Recovery:

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

31110 - Database audit fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbAuditFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact *My Oracle Support (MOS)*.

31111 - Database merge audit in progress

Alarm Group: COLL

Description: Database Merge Audit between mate nodes in progress

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMergeAuditNotify

Recovery:

No action required.

31112 - Stateful db synchronization from mate server

Alarm Group: REPL

Description: Stateful database is not yet synchronized with mate database.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 30

OID: comcolDbRepUpLogTransTimeoutNotify

Recovery:

No action required. Contact *My Oracle Support (MOS)* if this occurs frequently.

31113 - DB replication manually disabled

Alarm Group: REPL

Description: DB Replication Manually Disabled

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolDbReplicationManuallyDisabledNotify

Recovery:

No action required.

31114 - DB replication over SOAP has failed

Alarm Group: REPL

Description: Database replication of configuration data via SOAP has failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 3600

OID: comcolDbReplicationSoapFaultNotify

Recovery:

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

31115 - Database service fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbServiceFaultNotify

Recovery:

1. Export event history for the given server and idbsvc task.
2. Contact *My Oracle Support (MOS)*.

31116 - Excessive shared memory

Alarm Group: MEM

Description: The amount of shared memory consumed exceeds configured thresholds

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolExcessiveSharedMemoryConsumptionNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31117 - Low disk free

Alarm Group: DISK

Description: The amount of free disk is below configured thresholds

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolLowDiskFreeNotify

Recovery:

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

31118 - Database disk store fault

Alarm Group: DISK

Description: Writing the database to disk failed

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbDiskStoreFaultNotify

Recovery:

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

31119 - Database updatelog overrun

Alarm Group: DB

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpdateLogOverrunNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31120 - Database updatelog write fault

Alarm Group: DB

Description: A Database change cannot be stored in the updatelog

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpdateLogWriteFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31121 - Low disk free early warning

Alarm Group: DISK

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolLowDiskFreeEarlyWarningNotify

Recovery:

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

31122 - Excessive shared memory early warning

Alarm Group: MEM

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31123 - Database replication audit command complete

Alarm Group: REPL

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

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepAuditCmdCompleteNotify

Recovery:

No action required.

31124 - ADIC error

Alarm Group: REPL

Description: An ADIC detected errors

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepAuditCmdErrNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31125 - Database durability degraded

Alarm Group: REPL

Description: Database durability has dropped below configured durability level

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbDurabilityDegradedNotify

Recovery:

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

31126 - Audit blocked

Alarm Group: REPL

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolAuditBlockedNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31127 - DB Replication Audit Complete

Alarm Group: REPL

Description: DB replication audit completed

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbRepAuditCompleteNotify

Recovery:

No action required.

31128 - ADIC Found Error

Alarm Group: REPL

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbADICErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31129 - ADIC Found Minor Issue

Alarm Group: REPL

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 14400

OID: comcolDbADICWarn

Recovery:

No action required.

31130 - Network health warning

Alarm Group: NET

Description: Network health issue detected

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolNetworkHealthWarningNotify

Recovery:

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

31131 - IDB Throttled for Extended Period

Alarm Group: DB

Description: IDB has one or more processes throttled for an extended period.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolOustedThrottleWarnNotify

Recovery:

1. Monitor for workload in excess of documented capacity.
2. Contact *My Oracle Support (MOS)* if this alarm persists.

31140 - Database perl fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbPerlFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31145 - Database SQL fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbSQLFaultNotify

Recovery:

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

31146 - DB mastership fault

Alarm Group: SW

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbMastershipFaultNotify

Recovery:

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

31147 - DB upsynclog overrun

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbUpSyncLogOverrunNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31148 - DB lock error detected

Alarm Group: DB

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolDbLockErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31200 - Process management fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcMgmtFaultNotify

Recovery:

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

31201 - Process not running

Alarm Group: PROC

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcNotRunningNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31202 - Unkillable zombie process

Alarm Group: PROC

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcZombieProcessNotify

Recovery:

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

31206 - Process mgmt monitoring fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcMgmtMonFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31207 - Process resource monitoring fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcResourceMonFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31208 - IP port server fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolPortServerFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31209 - Hostname lookup failed

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHostLookupFailedNotify

Recovery:

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

31213 - Process scheduler fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolProcSchedulerFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31214 - Scheduled process fault

Alarm Group: PROC

Description: A scheduled process cannot be executed or abnormally terminated

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolScheduleProcessFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31215 - Process resources exceeded

Alarm Group: SW

Description: A process is consuming excessive system resources

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 14400

OID: comcolProcResourcesExceededFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31216 - SysMetric configuration error

Alarm Group: SW

Description: A SysMetric Configuration table contains invalid data

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolSysMetricConfigErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31220 - HA configuration monitor fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaCfgMonitorFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31221 - HA alarm monitor fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAlarmMonitorFaultNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31222 - HA not configured

Alarm Group: HA

Description: High availability is disabled due to system configuration

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaNotConfiguredNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31223 - HA Heartbeat transmit failure

Alarm Group: HA

Description: The high availability monitor failed to send heartbeat

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaHbTransmitFailureNotify

Recovery:

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

31224 - HA configuration error

Alarm Group: HA

Description: High availability configuration error

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID:comcolHaCfgErrorNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31225 - HA service start failure

Alarm Group: HA

Description: The high availability service failed to start

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaSvcStartFailureNotify

Recovery:

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

31226 - HA availability status degraded

Alarm Group: HA

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAvailDegradedNotify

Recovery:

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

31227 - HA availability status failed

Alarm Group: HA

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaAvailFailedNotify

Recovery:

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

31228 - HA standby offline

Alarm Group: HA

Description: High availability standby server is offline

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolHaStandbyOfflineNotify

Recovery:

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

31229 - HA score changed

Alarm Group: HA

Description: High availability health score changed

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaScoreChangeNotify

Recovery:

Status message - no action required.

31230 - Recent alarm processing fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolRecAlarmEvProcFaultNotify

Recovery:

1. Export event history for the given server and raclerk task.
2. Contact *My Oracle Support (MOS)*.

31231 - Platform alarm agent fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolPlatAlarmAgentNotify

Recovery:

Contact *My Oracle Support (MOS)*.

31232 - Late heartbeat warning

Alarm Group: HA

Description: High availability server has not received a heartbeat within the configured interval. High availability server has not received a message on specified path within the configured interval.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaLateHeartbeatWarningNotify

Recovery:

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

31233 - HA Secondary Path DownHA Path Down

Alarm Group: HA

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

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaPathDownNotify

Recovery:

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

31234 - Untrusted Time Upon Initialization

Alarm Group: REPL

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: comcolUtrustedTimeOnInitNotify

Recovery:

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

31235 - Untrusted Time After Initialization

Alarm Group: REPL

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

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0

OID: comcolUtrustedTimePostInitNotify

Recovery:

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

31236 - HA Link Down

Alarm Group: HA

Description: High availability TCP link is down.

Severity: Critical

Instance: Remote node being connected to plus the path identifier

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaLinkDownNotify

Recovery:

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

31240 - Measurements collection fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID:comcolMeasCollectorFaultNotify

Recovery:

1. Export event history for the given server and statclerk task.
2. Contact *My Oracle Support (MOS)*.

31250 - RE port mapping fault

Alarm Group: SW

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolRePortMappingFaultNotify

Recovery:

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

31260 - Database SNMP Agent

Alarm Group: SW

Description: The Database SNMP agent (snmpIdbAgentcmsnmpa) is impaired by a s/w fault

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: sdsDbcomcolSnmpAgentNotify

Recovery:

1. Export event history for the given server and all processes.
2. Contact *My Oracle Support (MOS)*.

31270 - Logging output

Alarm Group: SW

Description: Logging output set to Above Normal

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolLoggingOutputNotify

Recovery:

Extra diagnostic logs are being collected, potentially degrading system performance. Contact *My Oracle Support (MOS)*.

31280 - HA Active to Standby transition

Alarm Group: HA

Description: HA active to standby activity transition

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolActiveToStandbyTransNotify

Recovery:

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

31281 - HA Standby to Active transition

Alarm Group: HA

Description: HA standby to active activity transition

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolStandbyToActiveTransNotify

Recovery:

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

31282 - HA Management Fault

Alarm Group: HA

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaMgmtFaultNotify

Recovery:

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

31283 - HA Server Offline

Alarm Group: HA

Description: High availability server is offline

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0

OID: comcolHaServerOfflineNotify

Recovery

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

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Group: HA

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

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRemoteHeartbeatWarningNotify

Recovery:

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

31285 - HA Split Brain Recovery Entry

Alarm Group: HA

Description: High availability split brain recovery entered

Severity: Info

Instance: Cluster set key of the DC outputting the event

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaSbrEntryNotify

Recovery:

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

31286 - HA Split Brain Recovery Plan

Alarm Group: HA

Description: High availability split brain recovery plan

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaSbrPlanNotify

Recovery:

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

31287 - HA Split Brain Recovery Complete

Alarm Group: HA

Description: High availability split brain recovery complete

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaSbrCompleteNotify

Recovery:

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

31290 - HA Process Status

Alarm Group: HA

Description: HA manager (cmha) status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaProcessStatusNotify

Recovery:

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

31291 - HA Election Status

Alarm Group: HA

Description: HA DC Election status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaElectionStatusNotify

Recovery:

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

31292 - HA Policy Status

Alarm Group: HA

Description: HA Policy plan status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaPolicyStatusNotify

Recovery:

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

31293 - HA Resource Link Status

Alarm Group: HA

Description: HA ResourceAgent Link status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaLinkStatusNotify

Recovery:

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

31294 - HA Resource Status

Alarm Group: HA

Description: HA Resource registration status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaResourceStatusNotify

Recovery:

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

31295 - HA Action Status

Alarm Group: HA

Description: HA Resource action status

Severity: Info

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaActionStatusNotify

Recovery:

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

31296 - HA Monitor Status

Alarm Group: HA

Description: HA Monitor action status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaMonitorStatusNotify

Recovery:

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

31297 - HA Resource Agent Info

Alarm Group: HA

Description: HA Resource Agent Info

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaInfoNotify

Recovery:

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

31298 - HA Resource Agent Detail

Alarm Group: HA

Description: Resource Agent application detailed information

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaRaDetailNotify

Recovery:

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

31299 - HA Notification Status

Alarm Group: HA

Description: HA Notification status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaNotificationNotify

Recovery:

No action required.

31300 - HA Control Status

Alarm Group: HA

Description: HA Control action status

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 300

OID: comcolHaControlNotify

Recovery:

No action required.

32100 - Breaker Panel Feed Unavailable

Alarm Group: PLAT

Description: Breaker Panel Breaker Unavailable

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlFeedUnavailable

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Group: PLAT

Description: Breaker Panel Breaker Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlBreakerFailure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

Alarm Group: PLAT

Description: Breaker Panel Monitoring Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlMntFailureNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32103 - Power Feed Unavailable

Alarm Group: PLAT

Description: Power Feed Unavailable

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerFeedUnavail

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Group: PLAT

Description: Power Supply 1 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply1Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Group: PLAT

Description: Power Supply 2 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply2FailureNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group: PLAT

Description: Power Supply 3 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply3FailureNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32107 - Raid Feed Unavailable

Alarm Group: PLAT

Description: Raid Feed Unavailable

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidFeedUnavailableNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Group: PLAT

Description: Raid Power 1 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidPower1Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Group: PLAT

Description: Raid Power 2 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidPower2Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Group: PLAT

Description: Raid Power 3 Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRaidPower3Failure

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32111 - Device Failure

Alarm Group: PLAT

Description: Device Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceFailure

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

32112 - Device Interface Failure

Alarm Group: PLAT

Description: Device Interface Failure

Severity: Critical

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDeviceIfFailureNotify

Recovery:

Contact *My Oracle Support (MOS)* to request hardware replacement.

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: sdsTpdEccUncorrectableErrorNotify

Recovery

Contact *My Oracle Support (MOS)* 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: sdsTpdSNMPGetFailureNotify

Recovery

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

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Type: 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: eagleXgDsrTpdNTPDaemonNotSynchronizedFailureNotify

Recovery:

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

32116 - TPD Server's Time Has Gone Backwards

Alarm Type: 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: eagleXgDsrTpdNTPTimeGoneBackwardsNotify

Recovery:

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

32117 - TPD NTP Offset Check Failure

Alarm Type: 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: eagleXgDsrNtpOffsetCheckFailureNotify

Recovery:

1. Run syscheck in verbose mode.

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

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: sdsTpdFanErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdIntDiskErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdRaidDiskErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdPlatformErrorNotify

Recovery

Contact *My Oracle Support (MOS)* 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: sdsTpdFileSystemErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdPlatProcessErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

32306 – Server RAM shortage error

Alarm Group: PLAT

Not Implemented.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdRamShortageError

Contact *My Oracle Support (MOS)*.

32307 - Server swap space shortage failure

Alarm 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: sdsTpdSwapSpaceShortageErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdProvNetworkErrorNotify

Recovery

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

32309 - Eagle Network A Error

Alarm Group: PLAT

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

Default Severity: Critical

OID: eagleXgDsrTpdEagleNetworkAErrorNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32310 - Eagle Network B Error

Alarm Group: PLAT

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

Default Severity: Critical

OID: eagleXgDsrTpdEagleNetworkBErrorNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

32311 - Sync Network Error

Alarm Group: PLAT

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

Default Severity: Critical

OID: eagleXgDsrTpdSyncNetworkErrorNotify

Recovery

Contact *My Oracle Support (MOS)* to request hardware replacement.

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: sdsTpdDiskSpaceShortageErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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

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: eagleXgDsrTpdDefaultRouteNetworkErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdTemperatureErrorNotify

Recovery

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

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

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

32315 – Server mainboard voltage error

Alarm Type: 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: sdsTpdMainboardVoltageErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdPowerFeedErrorNotify

Recovery

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

32317 - Server disk health test error

Alarm Type: 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: sdsTpdDiskHealthErrorNotify

Recovery

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

32318 - Server disk unavailable error

Alarm Type: 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: sdsTpdDiskUnavailableErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdDeviceErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdDeviceIfErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdEccCorrectableErrorNotify

Recovery

No recovery necessary. If the condition persists, contact *My Oracle Support (MOS)* 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: sdsTpdPowerSupply1ErrorNotify

Recovery

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

32323 – Power Supply B error

Alarm Type: 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: sdsTpdPowerSupply2ErrorNotify

Recovery

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

32324 – Breaker panel feed error

Alarm Type: 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: sdsTpdBrkPnlFeedErrorNotify

Recovery

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

32325 - Breaker panel breaker error

Alarm Type: 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 15: Breaker Panel LEDs*) identify whether the fault occurred on the input power or the output power, as follows:

- A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit.

  Note: LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.

- A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.

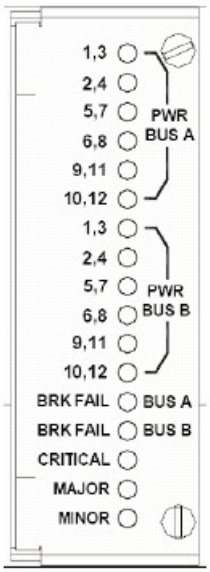


Figure 15: Breaker Panel LEDs

Description: This alarm indicates that a power fault has been identified by the breaker panel.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdBrkPnlBreakerErrorNotify

Recovery

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

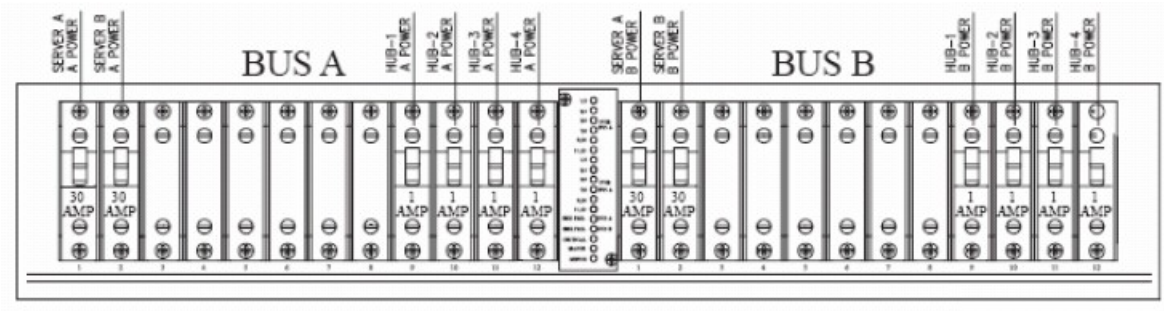


Figure 16: Breaker Panel Setting

If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Contact the *My Oracle Support (MOS)*

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 *My Oracle Support (MOS)*

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

- If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise Contact the *My Oracle Support (MOS)*

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 *My Oracle Support (MOS)*

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
- 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: sdsTpdBrkPnlMntErrorNotify

Recovery

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

32327 – Server HA Keepalive error

Alarm Type: 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: sdsTpdHaKeepaliveErrorNotify

Recovery

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

   Note: This step may require command line ability.

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

32328 – DRBD is unavailable

Alarm Group: PLAT

Description: This alarm indicates that DRBD is not functioning properly on the local server. The DRBD state (disk state, node state, and/or connection state) indicates a problem.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdUnavailable

Recovery

Contact *My Oracle Support (MOS)*.

32329 – DRBD is not replicating

Alarm Group: PLAT

Description: This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.

Severity: Major

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdDrbdNotReplicating

Recovery

Contact *My Oracle Support (MOS)*.

32330 – DRBD peer problem

Alarm Type: PLAT

Description: This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.

Severity: Major

OID: eagleXgDsrTpdDrbdPeerProblemNotify

Recovery

Contact the *My Oracle Support (MOS)*.

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: sdsTpdHpDiskProblemNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdHpDiskCtrlrProblemNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdHPACUCLIProblemNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdMpathDeviceProblemNotify

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: sdsTpdSwitchLinkDownErrorNotify

Recovery

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

32336– Half Open Socket Limit

Alarm Type: 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: sdsTpdHalfOpenSockLimitNotify

Recovery

Contact *My Oracle Support (MOS)*.

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 *My Oracle Support (MOS)*.

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 *My Oracle Support (MOS)*.

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: eagleXgDsrTpdMaxPidLimitNotify

Recovery:

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

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: eagleXgDsrTpdNTPDaemonNotSynchronizedErrorNotify

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. Contact *My Oracle Support (MOS)*.

32341 - Server NTP Daemon Never Synchronized Error

Alarm 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: eagleXgDsrTpdNTPDaemonNeverSynchronizedNotify

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
2. Contact *My Oracle Support (MOS)*.

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: eagleXgDsrNtpOffsetCheckErrorNotify

Recovery:

1. Verify NTP settings and that NTP are providing accurate time.
2. Contact *My Oracle Support (MOS)*.

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: eagleXgDsrTpdDiskProblemNotify

Recovery:

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

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: eagleXgDsrTpdDiskCtrlrProblemNotify

Recovery:

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

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: eagleXgDsrTpdUpgradeSnapshotInvalidNotify

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. Contact *My Oracle Support (MOS)*

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: sdsTpdDiskSpaceShortageWarningNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdApplicationProcessErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdHardwareConfigErrorNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: eagleXgDsrTpdRamShortageWarningNotify

Recovery

Contact *My Oracle Support (MOS)*.

32504 – Software Configuration Error

Alarm Group: PLAT

Description: This alarm is generated by the MPS syscheck software package and is not part of the PLAT distribution.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdSoftwareConfigError

Recovery

Contact *My Oracle Support (MOS)*.

32505 – Server swap space shortage warning

Alarm 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: sdsTpdSwapSpaceShortageWarningNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdDefaultRouteNotDefinedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdTemperatureWarningNotify

Recovery

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

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

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

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

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

32508 – Server core file detected

Alarm Type: 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: sdsTpdCoreFileDetectedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdNTPDeamonNotSynchronizedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdCMOSBatteryVoltageLowNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdSmartTestWarnNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdDeviceWarnNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdDeviceIfWarnNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdWatchdogRebootNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdHaInhibitedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdHaActiveToStandbyTransNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdHaStandbyToActiveTransNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdPlatformHealthCheckFailedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsNtpOffsetCheckFailedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsNtpStratumCheckFailedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsSasPresenceSensorMissingNotify

Recovery

Contact *My Oracle Support (MOS)* 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: sdsSasDriveMissingNotify

Recovery

Contact *My Oracle Support (MOS)* 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: eagleXgDsrTpdDrbdFailoverBusyNotify

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 *My Oracle Support (MOS)*.

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 dependent on the size of the disk and the amount of activity on the system.

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: sdsTpdHpDiskResyncNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: eagleXgDsrTpdTelcoFanWarningNotify

Recovery

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

32526 – Telco Temperature Warning

Alarm 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: eagleXgDsrTpdTelcoTemperatureWarningNotify

Recovery

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

32527 – Telco Power Supply Warning

Alarm Type: 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: eagleXgDsrTpdTelcoPowerSupplyWarningNotify

Recovery

1. Verify breaker wasn't tripped.
2. If breaker is still good and problem persists, contact *My Oracle Support (MOS)* who can perform a **snmpget** command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 – Invalid BIOS value

Alarm Type: 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: sdsTpdInvalidBiosValueNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdServerKernelDumpFileDetectedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: sdsTpdServerUpgradeFailDetectedNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: eagleXgDsrTpdHalfOpenSocketWarningNotify

Recovery

Contact *My Oracle Support (MOS)*.

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: eagleXgDsrTpdServerUpgradePendingAcceptNotify

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: eagleXgDsrTpdMaxPidWarningNotify

Recovery:

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

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: eagleXgDsrTpdNTPSourceIsBadNotify

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
2. Contact *My Oracle Support (MOS)*.

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 dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity: Minor

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

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: eagleXgDsrTpdDiskResyncNotify

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 *My Oracle Support (MOS)*.

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: eagleXgDsrTpdUpgradeSnapshotWarningNotify

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. Contact *My Oracle Support (MOS)*

32700 - Telco Switch Notification

Alarm Group: PLAT

Description: Telco Switch Notification

Severity: Info

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

HA Score: Normal

Auto Clear Seconds: 30

OID: tpdTelcoSwitchNotification

Recovery

Contact *My Oracle Support (MOS)*.

Chapter 5

Key Performance Indicators (KPIs)

Topics:

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

General KPIs information

This section provides general information about KPIs, the Status and Manage KPI page, and how to view KPIs.

KPIs overview

Key Performance Indicators (KPIs) allow the user to monitor system performance data, including CPU, memory, swap space, and uptime per server. This performance data is collected from all servers within the defined topology.

The KPI display function resides on all OAM servers. Servers that provide a GUI connection rely on KPI information merged to that server. The Network OAMP servers maintain status information for all servers in the topology. System OAM servers have reliable information only for servers within the same network element.

The Status and Manage KPIs page displays performance data for the entire system. KPI data for the entire system is updated every 60 seconds. If data is not currently being collected for a particular server, the KPI for that server will be shown as Unk for "Unknown".

KPIs

The **Status & Manage > KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAMP server or an SOAM server.

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 15: 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 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*

KPIs server elements

This table describes KPIs that appear regardless of server role.

Table 16: KPIs Server Elements

KPIs Status Element	Description
Network Element	The network element name (set up on the **Configuration > Network Elements** page) associated with each Server Hostname.

KPIs Status Element	Description
Server Hostname	The server hostname set up on the **Configuration > Servers** page. All servers in the system are listed here.
Server Indicators:	
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system.
RAM	Percentage utilization of physical memory on the server by all software as measured by TPD.
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.
Uptime	The total amount of time the server has been running.

Provisioning KPIs

Table 17: provisioning KPIs

Variable	Description
ProvConnections	The number of provisioning client connections currently established. A single connection includes a client having successfully established a TCP/IP connection, sent a provisioning connect message, and having received a successful response.
ProvMsgsReceived	The number of provisioning messages per second that have been received from all sources except import files.
ProvMsgsImported	The number of provisioning messages per second imported from files.
ProvMsgsSuccessful	The number of provisioning messages per second that have been successfully processed and a success response sent to the requestor.
ProvMsgsFailed	The number of provisioning messages per second that have failed to be processed due to errors and a failure response sent to the requestor.
ProvMsgsSent	The number of provisioning message responses sent per second to the requestor.
ProvMsgsDiscarded	The number of provisioning messages discarded per second. provisioning messages are discarded

Variable	Description
	due to connection shutdown, server shutdown, server's role switching from active to standby, or transaction not becoming durable within the allowed amount of time.
ProvTxnCommitted	The number of provisioning transactions per second that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS cluster.
ProvTxnFailed	The number of provisioning transactions per second that have failed to be started, committed, or aborted due to errors.
ProvTxnAborted	The number of provisioning transactions aborted per second.
ProvTxnActive	The number of provisioning transactions that are currently active (normal transaction mode only).
ProvTxnNonDurable	The number of transactions that have been committed, but are not yet durable. Responses for the associated requests are not sent until the transaction has become durable.
ProvRelayMsgsSent	The number of relayed provisioning messages sent per second.
ProvRelayMsgsSuccessful	The number of relayed provisioning messages per second that were successful at the HLRR.
ProvRelayMsgsFailed	The number of relayed provisioning messages per second that failed at the HLRR.
ProvRemoteAuditMsgsSent	The number of IMSI and MSISDN records audited per second.
ProvRelayTimeLag	Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.

Process-based KPIs

Table 18: Process-based KPIs

Variable	Description
provimport.Cpu	CPU usage of provimport process
provimport.MemHeap	Heap memory usage of provimport process
provimport.MemBasTotal	Memory usage of provimport process

Variable	Description
provimport.MemPerTotal	Percent memory usage of provimport process
provexport.Cpu	CPU usage of provexport process
provexport.MemHeap	Heap memory usage of provexport process
provexport.MemBasTotal	Memory usage of provexport process
provexport.MemPerTotal	Percent memory usage of provexport process
pdbrelay.Cpu	CPU usage of pdbrelay process
pdbrelay.MemHeap	Heap memory usage of pdbrelay process
pdbrelay.MemBasTotal	Memory usage of the pdbrelay process
pdbrelay.MemPerTotal	Percent memory usage of pdbrelay process
pdbaudit.Cpu	CPU usage of pdbaudit process
pdbaudit.MemHeap	Heap memory usage of pdbaudit process
pdbaudit.MemBasTotal	Memory usage of the pdbaudit process
pdbaudit.MemPerTotal	Percent memory usage of pdbaudit process
pdba.Cpu	CPU usage of pdba process
pdba.MemHeap	Heap memory usage of pdba process
pdba.MemBasTotal	Memory usage of pdba process
pdba.MemPerTotal	Percent memory usage of pdba process
xds.Cpu	CPU usage of xds process
xds.MemHeap	Heap memory usage of xds process
xds.MemBasTotal	Memory usage of xds process
xds.MemPerTotal	Percent memory usage of xds process
dpserver.Cpu	CPU usage of dpserver process on DP
dpserver.MemHeap	Heap memory usage of dpserver process on DP
dpserver.MemBaseTotal	Memory usage of the dpserver process on DP
dpserver.MemPerTotal	Percent memory usage of dpserver on DP
era.Cpu	CPU usage of era process
era.MemHeap	Heap memory usage of era process
era.MemBasTotal	Memory usage of era process
era.MemPerTotal	Percent memory usage of era process

DP KPIs

Table 19: DP KPIs

Variable	Description
DpsQueryRate	Total number of queries received per second
DpsMsisdnQueryRate	Total number of MSISDN queries received per second
DpsImsiQueryRate	Total number of IMSI queries received per second
DpsNaiQueryRate	Total number of NAI queries received per second
DpsFailedQueryRate	Total number of queries failed per second
DpsNotFoundQueryRate	Total number of queries with Not Found responses per second
DpsMsisdnNotFoundQueryRate	Total number of MSISDN queries with Not Found responses per second
DpsImsiNotFoundQueryRate	Total number of IMSI queries with Not Found responses per second
DpsNaiNotFoundQueryRate	Total number of NAI queries with Not Found responses per second
DpsResponseSent	Total number of responses sent per second
DpsIngressQueue	DP Ingress Queue percentage full
DpsMsisdnBlacklistedRate	Total number of MSISDN Queries with Blacklisted Responses per second
DpsImsiBlacklistedRate	Total number of IMSI Queries with Blacklisted Responses per second

Communication Agent (ComAgent) KPIs

The KPI values associated with ComAgent are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 20: 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

Variable	Description
	Data StackEvents (messages) that ComAgent delivers to Application Layers Queue.

Chapter 6

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 21: 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 22: 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*

Provisioning interface measurements

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

Table 23: Application Routing Rule Measurements

Measurement Tag	Description	Collection Interval
ProvConnectsAttempted	The total number of client initiated connect attempts to	5 min

Measurement Tag	Description	Collection Interval
	establish a connection with the server.	
ProvConnectsAccepted	The total number of client initiated connect attempts that have been accepted.	5 min
ProvConnectsDenied	The total number of client initiated connect attempts that have been denied due to clients not running on an authorized server, maximum number of allowed connections already established, or the provisioning interface is disabled.	5 min
ProvConnectsFailed	The total number of client initiated connect attempts that failed due to errors during initialization.	5 min
ProvConnectionIdleTimeouts	The total number of connections that have timed out and terminated due to idleness.	5 min
ProvMsgsReceived	The total number of provisioning messages that have been received from all sources (except import files).	5 min
ProvMsgsSuccessful	The total number of provisioning messages that have been successfully processed and a success response sent to the requestor.	5 min
ProvMsgsFailed	The total number of provisioning messages that have failed to be processed due to errors and a failure response sent to the requestor.	5 min
ProvMsgsSent	The total number of provisioning messages for which a response has been sent to the requestor.	5 min
ProvMsgsDiscarded	The total number of provisioning messages that have been discarded (instead of sending a reply to the requestor) due to the connection being shutdown, server being shutdown, server's role switching from active to	5 min

Measurement Tag	Description	Collection Interval
	standby, or transaction not becoming durable within the allowed amount of time.	
ProvMsgsImported	The total number of provisioning messages that have been received from a file import operation.	5 min
ProvTxnCommitted	The total number of transactions that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS site.	5 min
ProvTxnWriteMutexTimeouts	The total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.	5 min
ProvTxnFailed	The total number of transactions that have failed to be started, committed, or aborted due to errors.	5 min
ProvTxnAborted	The total number of transactions that have been successfully aborted.	5 min
ProvTxnTotal	The total number of transactions that have been attempted. It is the sum of ProvTxnCommitted, ProvTxnTimeouts, ProvTxnAborted, and ProvTxnFailed counters.	5 min
ProvTxnDurabilityTimeouts	The total number of committed, non-durable transaction that have failed to become durable within the amount of time specified by Transaction Durability Timeout.	5 min
RemoteAuditStarted	Number of started remote audit requests.	5 min
RemoteAuditCompleted	Number of successfully completed remote audit requests.	5 min
ProvRelayMsgsSent	The total number of relayed provisioning messages sent to the remote system.	5 min

Measurement Tag	Description	Collection Interval
ProvRelayMsgsSuccessful	The total number of relayed provisioning messages that have been successfully processed on the remote system.	5 min
ProvRelayMsgsFailed	The total number of relayed provisioning messages that have failed to be processed due to errors on the remote system.	5 min
ProvImportsSuccessful	The number of files imported successfully.	5 min
ProvImportsFailed	The number of files that failed to be imported due to errors.	5 min
ProvExportsSuccessful	The number of successful file export requests.	5 min
ProvExportsFailed	The number of file export requests that failed due to errors.	5 min
ProvDnSplitCreated	Number of MSISDN records successfully created by a Split Activation starting its PDP.	5 min
ProvDnSplitRemoved	Number of MSISDN records successfully removed by a Split Completing its PDP.	5 min
ProvNpaSplitStarted	Number of NPA split records successfully starting a PDP.	5 min
ProvNpaSplitCompleted	Number of NPA split records successfully completing a PDP.	5 min
ProvRemoteAuditMsgsSent	Number of IMSI and MSISDN records audited.	5 min
ProvRelayTimeLag	Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.	5 min

ProvConnectsAttempted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of client initiated connect attempts to establish a connection with the server.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvConnectsAccepted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of client initiated connect attempts that have been accepted.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvConnectsDenied

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of client initiated connect attempts that have been denied due to clients not running on an authorized server, maximum number of allowed connections already established, or the provisioning interface is disabled.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvConnectsFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

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

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvConnectionIdleTimeouts

Measurement Group: Provisioning Rules

Measurement Type: Simple

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

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvMsgsReceived

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of PROVISIONING messages that have been received from all sources (except import files).

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvMsgsImported

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of PROVISIONING messages that have been received from a file import operation.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvMsgsSuccessful

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of PROVISIONING messages that have been successfully processed and a success response sent to the requestor.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvMsgsFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of PROVISIONING messages that have failed to process due to errors and a failure response sent to the requestor.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvMsgsSent

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of PROVISIONING messages that have been sent and a response sent to the requestor.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvMsgsDiscarded

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of PROVISIONING messages that have been discarded (instead of sending a reply to the requestor) due to the connection being shutdown, server being shutdown, server's role switching from active to standby, or transaction not becoming durable within the allowed amount of time.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnCommitted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of transactions that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS site.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnWriteMutexTimeouts

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of write transactions that have failed to be processed due to timing out while waiting to acquire the write transaction mutex.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of transactions that have failed to be started, committed, or aborted due to errors.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnAborted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of transactions that have been successfully aborted.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnDurabilityTimeouts

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of committed, non-durable transaction that have failed to become durable within the amount of time specified by Transaction Durability Timeout.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvTxnTotal

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of transactions that have been attempted. It is the sum of ProvTxnCommitted, ProvTxnTimeouts, ProvTxnAborted, and ProvTxnFailed counters.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvImportsSuccessful

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The number of files imported successfully.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvImportsFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The number of files that failed to be imported due to errors.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvExportsSuccessful

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The number of successful CSV/XML file export requests.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvExportsFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The number of CSV/XML file export requests that failed due to errors.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvDnSplitCreated

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of DN records successfully created by an Active Split.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvDnSplitRemoved

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of DN records successfully removed by a Split Completing its PDP.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvNpaSplitStarted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of NPA split records successfully starting a PDP.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvNpaSplitCompleted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of NPA split records successfully completing a PDP.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvRelayMsgsFailed

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of relayed PROVISIONING messages that have failed to be processed due to errors on the remote system.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvRelayMsgsSent

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of relayed PROVISIONING messages sent to the remote system.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvRelayMsgsSuccessful

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: The total number of relayed PROVISIONING messages that have been successfully processed on the remote system.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvRelayTimeLag

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

ProvRemoteAuditMsgsSent

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of IMSI and MSISDN records audited.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

RemoteAuditCompleted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of successfully completed remote audit requests.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

RemoteAuditStarted

Measurement Group: Provisioning Rules

Measurement Type: Simple

Description: Number of started remote audit requests.

Collection Interval: 5 min

Peg Condition:

Measurement Scope: PROV Group

Recovery:

No action required.

DP Measurements

Table 24: DP Measurements

Measurement Tag	Description	Collection Interval
DpsQueriesReceived	Number of Queries received	5 minutes
DpsMsisdnQueriesReceived	Number of MSISDN Queries received	5 minutes
DpsImsiQueriesReceived	Number of IMSI Queries received	5 minutes
DpsNaiQueriesReceived	Number of NAI Queries received	5 minutes
DpsQueriesFailed	Number of Queries failed	5 minutes
DpsMsisdnQueriesFailed	Number of MSISDN Queries with Fail response	5 minutes
DpsImsiQueriesFailed	Number of IMSI Queries with Fail response	5 minutes
DpsNaiQueriesFailed	Number of NAI Queries with Fail response	5 minutes
DpsSuccessResponses	Number of Queries with Success response	5 minutes
DpsMsisdnSuccessResponses	Number of MSISDN Queries with Success response	5 minutes
DpsImsiSuccessResponses	Number of IMSI Queries with Success response	5 minutes
DpsNaiSuccessResponses	Number of NAI Queries with Success response	5 minutes
DpsNotFoundReponses	Number of Queries with Not Found response	5 minutes
DpsMsisdnNotFoundResponses	Number of MSISDN Queries with Not Found response	5 minutes
DpsImsiNotFoundResponses	Number of IMSI Queries with Not Found response	5 minutes
DpsNaiNotFoundResponses	Number of NAI Queries with Not Found response	5 minutes
DpsRespSent	Total number of responses sent	5 minutes
DpsIngressQueuePeak	Peak DPS Ingress Queue utilization during collection period	5 minutes
DpsIngressQueueAvg	Average DPS Ingress Queue utilization during the collection period	5 minutes
DpsIngressQueueFull	Number of DPS Ingress Queue StackTask messages discarded during the collection	5 minutes

Measurement Tag	Description	Collection Interval
	period because the number of message queued exceeded the maximum capacity	
DpsQueryRatePeak	Peak Ingress Message Rate in messages per second during the collection period	5 minutes
DpsQueryRateAvg	Average Ingress Message Rate in messages per second during the collection period	5 minutes
DpsQueryProcessingTime	Distribution of times (in microseconds) taken by dpserver to process each query and send its reply.	5 minutes
DpsQueryProcessingTimeAvg	The average query processing time (in microseconds) taken by dpserver to process each query and sent its reply.	5 minutes
DpsMsisdnBlacklistedResponses	Number of MSISDN Queries with Blacklisted response	5 minutes
DpsImsiBlacklistedResponses	Number of IMSI Queries with Blacklisted response	5 minutes
DpsMsisdnPrefixFound	Number of MSISDN Queries that were found by matching a prefix	5 minutes
DpsImsiPrefixFound	Number of IMSI Queries that were found by matching a prefix	5 minutes
DpsMsisdnBlacklistLookups	Number of MSISDN Blacklist Lookups performed	5 minutes
DpsImsiBlacklistLookups	Number of IMSI Blacklist Lookups performed	5 minutes
DpsMsisdnPrefixLookups	Number of MSISDN Prefix Lookups performed	5 minutes
DpsImsiPrefixLookups	Number of IMSI Prefix Lookups performed	5 minutes

DpsQueriesReceived

Measurement Group: DP

Measurement Type: Simple

Description: Number of Queries received

Collection Interval: 5 min

Peg Condition:

Measurement Scope: DP Group

Recovery:

No action required.

DpsMsisdnQueriesReceived

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Queries received

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiQueriesReceived

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Queries received

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsNaiQueriesReceived

Measurement Group: DP

Measurement Type: Simple

Description: Number of NAI Queries received

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsQueriesFailed

Measurement Group: DP

Measurement Type: Simple

Description: Number of Queries failed

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnQueriesFailed

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Queries with Fail response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiQueriesFailed

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Queries with Fail response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsNaiQueriesFailed

Measurement Group: DP

Measurement Type: Simple

Description: Number of NAI Queries with Fail response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsSuccessResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of Queries with Success response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnSuccessResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Queries with Success response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiSuccessResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Queries with Success response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsNaiSuccessResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of NAI Queries with Success response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsNotFoundResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of Queries with Not Found response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnNotFoundResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Queries with Not Found response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiNotFoundResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Queries with Not Found response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsNaiNotFoundResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of NAI Queries with Not Found response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsRespSent

Measurement Group: DP

Measurement Type: Simple

Description: Total number of responses sent

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsIngressQueuePeak

Measurement Group: DP

Measurement Type: Simple

Description: Peak DPS Ingress Queue utilization during collection period

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsIngressQueueAvg

Measurement Group: DP

Measurement Type: Simple

Description: Average DPS Ingress Queue utilization during collection period

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsIngressQueueFull

Measurement Group: DP

Measurement Type: Simple

Description: Number of DPS Ingress Queue Stack Task messages discarded during the collection period because the number of messages queued exceeded the maximum capacity

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsQueryRatePeak

Measurement Group: DP

Measurement Type: Simple

Description: Peak Ingress Message Rate in messages per second during the collection period

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsQueryRateAvg

Measurement Group: DP

Measurement Type: Simple

Description: Average Ingress Message Rate in messages per second during the collection period

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsQueryProcessingTime

Measurement Group: DP

Measurement Type: Simple

Description: Distribution of times (in microseconds) taken by dpserver to process each query and send its reply

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsQueryProcessingTimeAvg

Measurement Group: DP

Measurement Type: Simple

Description: The average query processing time (in microseconds) taken by dpserver to process each query and send its reply

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnBlacklistedResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Queries with Blacklisted response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiBlacklistedResponses

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Queries with Blacklisted response

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnPrefixFound

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Queries that were found by matching a prefix

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiPrefixFound

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Queries that were found by matching a prefix

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnBlacklistLookups

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Blacklist Lookups performed

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiBlacklistLookups

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Blacklist Lookups performed

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsMsisdnPrefixLookups

Measurement Group: DP

Measurement Type: Simple

Description: Number of MSISDN Prefix Lookups performed

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

DpsImsiPrefixLookups

Measurement Group: DP

Measurement Type: Simple

Description: Number of IMSI Prefix Lookups performed

Collection Interval: 5 min

Peg Condition:

Measurement Scope: Data Processor

Recovery:

No action required.

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 25: 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
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

Measurement Tag	Description	Collection Interval
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
CAPSTxGrpSuccess	Number of egress stack events successfully routed to a known Peer Group.	30 min
CAPSTxGrp	Number of egress stack events submitted to the PG Service to be routed to a known Peer Group.	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 ID: 9969

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed

Description: Average percentage of ComAgent DataFIFO Queue Utilization.

Collection Interval: 30 min

Peg Condition: The average ComAgent connection DataFIFO Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating any issues with ComAgent User Data StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

CAAvgMxFIFOQueueUtil

Measurement ID: 9967

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed

Description: Average percentage of ComAgent MxFIFO Queue Utilization.

Collection Interval: 30 min

Peg Condition: The average ComAgent connection MxFIFO Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating any issues with internal StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

CAAvgQueueUtil

Measurement ID: 9828

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed

Description: Average percentage of Queue Utilization.

Collection Interval: 30 min

Peg Condition: The average ComAgent Egress Task Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact *My Oracle Support (MOS)* for assistance.

CAAvgRsrcPoolUtil

Measurement ID: 9858

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Average percentage of internal resource pool utilization.

Collection Interval: 30 min

Peg Condition: This is to track the measure of average usage of the internal resource (Ex: CommMessage Resource pool) for a given interval.

Measurement Scope: NE, Server

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional processing or performance capacity tuning on a node.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of a node over several collection intervals, then the internal engineering resource pool capacity or other dependent parameters may need to be tuned, so that it does not result in unaccounted latency.

CAAvgRxStackEvents

Measurement ID: 9822

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Average Number of User Data ingress events received.

Collection Interval: 30 min

Peg Condition: The average User Data ingress StackEvent sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of Average Value during the interval, for number of User Data messages received from remote.

CAAvgTxStackEvents

Measurement ID: 9816

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Single

Description: Average Number of User Data egress events received from stacks to deliver it to remote.

Collection Interval: 30 min

Peg Condition: The average User Data egress StackEvent sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of Average Value during the interval, for number of User Data messages transmitted to remote.

CADSTx

Measurement ID: 9814

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events specifically for the default Direct Service.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent received specifically for the default Direct Service and processed by ComAgent Stack.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data egress messages are received by ComAgent to be transmitted from hosting server to destined remote server using default Direct "EventTransfer" Service.

CAHSTxRsrc

Measurement ID: 9876

Measurement Group: ComAgent Performance, ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of egress stack events that were routed to a known Resource.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Resource.

Measurement Scope: Server

Recovery:

No action required.

CAHSTxRsrcRateAvg

Measurement ID: 9877

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Resource ID)

Description: Average rate per second of egress stack events routed to a known Resource.

Collection Interval: 30 min

Peg Condition: Based upon the SysMetric.

Measurement Scope: Server

Recovery:

No action required.

CAHSTxRsrcRateMax

Measurement ID: 9878

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Resource ID)

Description: Maximum rate per second of egress stack events routed to a known Resource.

Collection Interval: 30 min

Peg Condition: Based upon the SysMetric.

Measurement Scope: Server

Recovery:

No action required.

CAPeakDataFIFOQueueUtil

Measurement ID: 9968

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Arrayed

Description: Maximum percentage of ComAgent DataFIFO Queue Utilization.

Collection Interval: 30 min

Peg Condition: The maximum ComAgent DataFIFO Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating any issues with ComAgent User Data StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

CAPeakMxFIFOQueueUtil

Measurement ID: 9966

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Arrayed

Description: Maximum percentage of ComAgent MxFIFO Queue Utilization.

Collection Interval: 30 min

Peg Condition: The maximum ComAgent connection MxFIFO Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating any issues with internal StackEvent processing and thread scheduling.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

CAPeakQueueUtil

Measurement ID: 9827

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Arrayed

Description: Maximum percentage of Queue Utilization.

Collection Interval: 30 min

Peg Condition: The maximum ComAgent Egress Task Queue utilization sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact *My Oracle Support (MOS)* for assistance.

CAPeakRsrcPoolUtil

Measurement ID: 9857

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Maximum percentage of internal resource pool utilization.

Collection Interval: 30 min

Peg Condition: This is to track the measure of maximum usage of the internal resource (Ex: CommMessage Resource pool) for a given interval.

Measurement Scope: NE, Server

Recovery:

This measurement is primarily intended to assist in evaluating the need for additional processing or performance capacity tuning on a node.

If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of a node over several collection intervals, then the internal engineering resource pool capacity or other dependent parameters may need to be tuned, so that it does not result in unaccounted latency.

CAPeakRxStackEvents

Measurement ID: 9821

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Maximum Number of User Data ingress events received.

Collection Interval: 30 min

Peg Condition: The maximum User Data ingress StackEvent sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of Peak Value during the interval, for number of User Data messages received from remote.

CAPeakTxStackEvents

Measurement ID: 9815

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Single

Description: Maximum Number of User Data egress events received from stacks to deliver it to remote.

Collection Interval: 30 min

Peg Condition: The maximum User Data egress StackEvent sample taken during the collection interval.

Measurement Scope: NE, Server

Recovery:

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 ID: 9844

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of stack events submitted to a Routed Service for routing.

Collection Interval: 30 min

Peg Condition: Stack event submitted to ComAgent Routed Service by a local User Layer

Measurement Scope: Server

Recovery:

No action necessary

CARx

Measurement ID: 9806

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data ingress events received from a peer server.

Collection Interval: 30 min

Peg Condition: For each User Data StackEvent received from one of the configured peer and processed by Communication Agent Stack.

Measurement Scope: NE, Server

Recovery:

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 ID: 9807

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data ingress events successfully routed to local layers.

Collection Interval: 30 min

Peg Condition: For each User Data StackEvent received from a peer server and successfully transmitted to the local stack.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data ingress messages are received by Communication Agent and are successfully transmitted to local hosting stack.

CATransEndAbnorm

Measurement ID: 9834

Measurement Group: ComAgent Exception, ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions that terminated abnormally.

Collection Interval: 30 min

Peg Condition:

- Transaction times-out waiting for a response, and the maximum number of transmits has been reached.
- Transaction time-to-live limit is exceeded.
- Transaction terminated due to lack of resources.

Note: This measurement is NOT pegged for these conditions:

- Transaction involves an unknown service.
- Transaction involves an unregistered Routed Service.

Measurement Scope: Server

Recovery:

1. Check the ComAgent Exception report to further diagnose the reasons why transactions are failing.
2. Contact *My Oracle Support (MOS)* for assistance.

CATransEndAbnormRateAvg

Measurement ID: 9865

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 ID: 9866

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 ID: 9836

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions initiated by local User Layers that ended normally with a response from a destination server.

Collection Interval: 30 min

Peg Condition: When a valid reliable response stack event (G=1, A=1) is received that corresponds to a pending transaction record.

Measurement Scope: Server

Recovery:

No action necessary.

This measurement has value when compared against other measurements. If no new transactions are started, then during normal operation, this measurement should match *CATransStarted* .

CATransPendingAvg

Measurement ID: 9838

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Service ID)

Description: Average number of allocated pending transaction records over the collection interval.

Collection Interval: 30 min

Peg Condition: Average number of allocated pending transaction records during the collection interval.

Measurement Scope: Server

Recovery:

No action necessary.

CATransPendingMax

Measurement ID: 9837

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Service ID)

Description: Maximum number of allocated pending transaction records.

Collection Interval: 30 min

Peg Condition: When a pending transaction record is allocated, and the total count of allocated pending transaction records exceeds the current peak.

Measurement Scope: Server

Recovery:

No action necessary.

CATransRateAvg

Measurement ID: 9863

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Service ID)

Description: Average rate per second that ComAgent transactions were started during the collection interval.

Collection Interval: 30 min

Peg Condition: Transaction rate monitoring is an average rate using 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 ID: 9864

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Service ID)

Description: Maximum rate per second that ComAgent transactions were started during the collection interval.

Collection Interval: 30 min

Peg Condition: Transaction rate monitoring is an average rate using 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 ID: 9835

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions initiated by local User Layers.

Collection Interval: 30 min

Peg Condition: When a valid reliable request stack event (G=1, R=1) is received from a local User Layer.

Measurement Scope: Server

Recovery:

No action necessary.

CATransTimeAvg

Measurement ID: 9840

Measurement Group: ComAgent Performance

Measurement Type: Average

Measurement Dimension: Arrayed (by Service ID)

Description: Average transaction life-time in milliseconds.

Collection Interval: 30 min

Peg Condition: Transaction ends either normally or abnormally.

Measurement Scope: Server

Recovery:

No action necessary.

CATransTimeMax

Measurement ID: 9839

Measurement Group: ComAgent Performance

Measurement Type: Max

Measurement Dimension: Arrayed (by Service ID)

Description: Maximum transaction life-time in milliseconds.

Collection Interval: 30 min

Peg Condition: Transaction ends either normally or abnormally.

Measurement Scope: Server

Recovery:

No action necessary.

CATx

Measurement ID: 9800

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events received on Communication Agent task queue from local stacks to deliver it to a peer server.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent received and processed by Communication Agent Stack.

Measurement Scope: NE, Server

Recovery:

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 ID: 9801

Measurement Group: ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events successfully delivered to a peer server.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent transmitted to the peer server.

Measurement Scope: NE, Server

Recovery:

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.

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 26: 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

Measurement Tag	Description	Collection Interval
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 Sub-Resource of a given Resource.	30 min
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
CAPSTxDscrdCongPeer	Number of egress events discarded because Peer congestion.	30 min
CAPSTxDscrdUnavailGrp	Number of egress stack events discarded because they referred to a Peer Group which was unavailable.	30 min
CAPSTxDscrdUnkwnGrp	Number of egress stack events discarded because they referred to a Peer Group which was unknown.	30 min
CARsrcPoolFul	ComAgent internal resource pool exhaustion condition	30 min
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

Measurement Tag	Description	Collection Interval
CARxDiscUnexpEvent	Number of ingress events discarded because it was unexpected in the connection operational state.	30 min
CARxDscrdBundle	Number of ingress bundled event discarded during de-serialization	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
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

Measurement Tag	Description	Collection Interval
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 response from a destination server.	30 min
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

Measurement Tag	Description	Collection Interval
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
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

Measurement Tag	Description	Collection Interval
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 ID: 9971

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: StackEvents discarded due to ComAgent DataFIFO queue full condition. This value provides a measure of how many messages are discarded by ComAgent due to ComAgent User Data FIFO Queue full condition.

Collection Interval: 30 min

Peg Condition: For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent User Data FIFO queue.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

CADSTxDscrdCong

Measurement ID: 9841

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of egress stack events discarded because the congestion level of the connection exceeded the stack events' priority level.

Collection Interval: 30 min

Peg Condition: When ComAgent receives a stack event from a local User Layer to be transferred via the direct service and the selected connection has a congestion level greater than the priority level of the stack event.

Measurement Scope: Server

Recovery:

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 *My Oracle Support (MOS)* for assistance.

CAHSRsrcErr

Measurement ID: 9875

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of times that ComAgent receives in a heartbeat stack event status concerning a known Resource but an unknown Sub-Resource.

Collection Interval: 30 min

Peg Condition: When ComAgent stores an unexpected Sub-Resource entry in the local Resource Provider Table. An unexpected Sub-Resource involves a known Resource but an unknown Sub-Resource ID (SRID). This condition is associated with Alarm-ID 19848, and only the first instance of an unexpected Sub-Resource is counted, not the repeats caused by multiple unknown Sub-Resources and the periodic heartbeats containing the same information.

Measurement Scope: Server

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** to determine configuration problems.
2. Contact *My Oracle Support (MOS)* for assistance.

CAHSTxDscrdIntErrSR

Measurement ID: 9874

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Sub-Resource and that is discarded due to a ComAgent internal error

Measurement Scope: Server

Recovery:

1. Check other ComAgent measurements, alarms, and events to determine the source of the abnormality causing this measurement to arise.
2. If the problem persists, contact *My Oracle Support (MOS)*.

CAHSTxDscrdCongSR

Measurement ID: 9872

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of stack events discarded due to HA Service Sub-Resource congestion. During normal operation, this measurement should not be increasing. When this measurement is increasing, it is an indication that the product is experiencing overload.

Collection Interval: 30 min

Peg Condition: Stack event submitted to ComAgent by a local User Layer, and the stack event references an HA Service Sub-Resource that has a congestion level greater than the priority level of the stack event.

Measurement Scope: Server

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to determine if the offered load is expected and exceeds the product's capacity.

   If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur. If the load does not exceed the 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 *My Oracle Support (MOS)* for assistance.

CAHSTxDscrdIntErrSR

Measurement ID: 9874

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of egress stack events destined to a known Sub-Resource that were discarded due to a ComAgent internal error.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Sub-Resource and that is discarded due to a ComAgent internal error

Measurement Scope: Server

Recovery:

1. Check other ComAgent measurements, alarms, and events to determine the source of the abnormality causing this measurement to arise.
2. If the problem persists, contact *My Oracle Support (MOS)*.

CAHSTxDscrdUnavailSR

Measurement ID: 9871

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of stack events discarded because they were submitted to an Unavailable Sub-Resource of a given Resource. During normal operation, this measurement should not be increasing. Each count of this measurement indicates that a local application attempted to send a stack event to another server using an HA Service Sub-Resource, but the event was discarded due to the Sub-Resource being unavailable.

Collection Interval: 30 min

Peg Condition: Stack event submitted to ComAgent by a local User Layer, and the stack event references an Unavailable Sub-Resource.

Measurement Scope: Server

Recovery:

1. Use **Main Menu** > **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 *My Oracle Support (MOS)* for assistance.

CAHSTxDscrdUnknownSR

Measurement ID: 9870

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of egress stack events discarded because they referred to a known Resource and an unknown Sub-Resource. During normal operation this measurement should be 0. A non-zero value for this measurement indicates that ComAgent is improperly configured to support a local application.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event that refers to an unknown Sub-Resource.

Measurement Scope: Server

Recovery:

1. Use **Main Menu** > **Comamunication Agent** > **Maintenance** > **HA Services Status** to verify that all HA Service Sub-Resources expected by local applications are present and operating.
2. Contact *My Oracle Support (MOS)* for assistance.

CAHSTxDscrdUnkwnRsrc

Measurement ID: 9873

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of egress stack events discarded because they referred to an unknown Resource.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event that refers to an unknown Resource.

Measurement Scope: Server

Recovery:

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

CAHSTxRsrc

Measurement ID: 9876

Measurement Group: ComAgent Performance, ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Resource ID)

Description: Number of egress stack events that were routed to a known Resource.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event destined to a known Resource.

Measurement Scope: Server

Recovery:

No action required.

CAMxFIFOQueueFul

Measurement ID: 9970

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: StackEvents discarded due to ComAgent MxFIFO queue full condition. This value provides a measure of how many messages are discarded by ComAgent due to ComAgent internal connection MxFIFO Queue full condition.

Collection Interval: 30 min

Peg Condition: For each User Data StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent internal connection MxFIFO queue.

Measurement Scope: NE, Server

Recovery:

1. This measurement is primarily intended to assist in evaluating the need for additional queue depth tuning or increase in processing capacity at a Network Element.

   If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the queue depth may need to be tuned.

   If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.

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

CARsrcPoolFul

Measurement ID: 9859

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: ComAgent internal resource pool exhaustion condition.

Collection Interval: 30 min

Peg Condition: This is to track the measure of the internal resource (Ex: CommMessage Resource pool) exhaustion condition for a given interval.

For each resource allocation/access attempt that result in resource pool manager returning an indication that the maximum resources reserved are allocated and are in-use. When this condition occurs ComAgent tries to allocate a new resource from heap and relists it after its life cycle (Ex: CommMessage objects required for user data traffic for MxEndpoint interface).

Measurement Scope: NE, Server

Recovery:

This value provides a measure of how many times pre-allocated resources are exhausted in ComAgent interfaces.

This measurement is primarily intended for performance analysis and to assist in evaluating the need for any additional engineering processing capacity or tuning.

CARSTxDscrdCong

Measurement ID: 9843

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of stack events discarded due to Routed Service congestion.

Collection Interval: 30 min

Peg Condition: Stack event submitted to ComAgent by a local User Layer, and the stack event references a Routed Service that has a congestion level greater than the priority level of the stack event.

Measurement Scope: Server

Recovery:

1. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Services Status** and **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screens to determine if the offered load is expected and exceeds the product's capacity.

If the load is expected and exceeds the product's capacity, then the capacity should be increased so that the overload condition does not persist or reoccur.

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

CARSTxDscrdInternalErr

Measurement ID: 9867

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of egress events discarded because of another Routed Service internal error

Collection Interval: 30 min

Peg Condition: Each time an egress event is discarded because of another Router Service internal error

Measurement Scope: Server

Recovery:

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

CARSTxDscrdSvcUnavail

Measurement ID: 9830

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of stack events discarded because they were submitted to an Unavailable Routed Service.

Collection Interval: 30 min

Peg Condition: Stack event submitted to ComAgent by a local User Layer, and the stack event references an Unavailable Routed Service.

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 *My Oracle Support (MOS)* for assistance.

CARxDiscUnexpEvent

Measurement ID: 9826

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded because it was unexpected in the connection operational state.

Collection Interval: 30 min

Peg Condition: For each ingress StackEvent that is discarded by ComAgent Stack, due to StackEvent received in unexpected connection state.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to message received in unexpected connection state.

CARxDscrdBundle

Measurement ID: 9994

Measurement Group: ComAgent Exception

Measurement Dimension: Single

Measurement Type: Simple

Description: Number of ingress bundled event discarded during routing.

Peg Condition: Each time an ingress bundled event is discarded during routing

Collection Interval: 30 min

Measurement Scope: Site

Recovery:

No action required

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 ID: 9810

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded because failed to deserialize (event not part of stack service language).

Collection Interval: 30 min

Peg Condition: For each StackEvent received from a configured peer server that resulted in any decode failures within ComAgent Stack.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to internal decode error condition.

CARxDscrdIncompat

Measurement ID: 9825

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded because an Incompatible header version is received.

Collection Interval: 30 min

Peg Condition: For each ingress StackEvent that is discarded by ComAgent Stack, due to unsupported base header version, as indicated in StackEvent.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to incompatible base header version of base software event library.

CARxDscrdInternalErr

Measurement ID: 9818

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded because of other unexpected internal processing error.

Collection Interval: 30 min

Peg Condition: For each ingress StackEvent that is discarded by ComAgent Stack, due to internal processing errors for conditions not covered by other meas-pegs.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to internal software processing errors for conditions not covered by other measurement pegs.

CARxDscrdLayerSendFail

Measurement ID: 9812

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data ingress events discarded because layer's sendTo failed.

Collection Interval: 30 min

Peg Condition: For each User Data StackEvent received from a configured service peer server and resulted in send failure to the destination stack layer.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data ingress messages are discarded by ComAgent due to internal send failure to destination stack layer.

CARxDscrdMsgLenErr

Measurement ID: 9808

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded as it doesn't contain enough bytes (less than event header bytes).

Collection Interval: 30 min

Peg Condition: For each StackEvent received from configured peer with message size less than the minimum required Header.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by Communication Agent due to message size error.

CARxDscrdUnkServer

Measurement ID: 9820

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded because the origination server was unknown/not configured.

Collection Interval: 30 min

Peg Condition: For each ingress StackEvent that is discarded by ComAgent Stack, due to unknown origination ip address contents in StackEvent.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent due to unknown origination ip address in StackEvent.

CARxDscrdUnkStkLyr

Measurement ID: 9811

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data ingress events discarded because stack layer is not known.

Collection Interval: 30 min

Peg Condition: For each User Data ingress StackEvent received by Communication Agent Stack, for an unknown destination stack.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by Communication Agent , as the destination stack is not registered/known.

CARxMsgUnknown

Measurement ID: 9809

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of ingress events discarded because stack event was unknown.

Collection Interval: 30 min

Peg Condition: For each undefined StackEvent received from one of the configured peer server.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many ingress messages are discarded by ComAgent as the message is not defined/known to ComAgent Stack.

CAStackQueueFul

Measurement ID: 9829

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed

Description: StackEvents discarded due to ComAgent task queue full condition.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent that is discarded by ComAgent Stack, due to failure in attempting to put the messages in ComAgent Egress Task Queue.

Measurement Scope: NE, Server

Recovery:

1. If both the peak and average measurement for multiple MPs within a Network Element are consistently near the recommended maximum engineered capacity of an MP over several collection intervals, then the number of MPs in the Network Element may need to be increased.
2. If the peak and average for an individual MP is significantly different than other MPs in the same Network Element then an MP-specific hardware, software, or configuration problem may exist.
3. Contact *My Oracle Support (MOS)* for assistance.

CATransDscrdInvCorrId

Measurement ID: 9832

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of received stack events that were received and discarded because they did not correlate with a pending transaction.

Collection Interval: 30 min

Peg Condition: ComAgent receives a response stack event that contains a correlation ID that does not match a pending transaction record.

Measurement Scope: Server

Recovery:

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 *My Oracle Support (MOS)* for assistance.

CATransDscrdStaleErrRsp

Measurement ID: 9833

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of times that an error response was discarded because it contained a valid correlation ID value but its originating server was not the last server to which the request was sent.

Collection Interval: 30 min

Peg Condition: ComAgent receives an error response stack event that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent.

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 *My Oracle Support (MOS)* for assistance.

CATransEndAbnorm

Measurement ID: 9834

Measurement Group: ComAgent Exception, ComAgent Performance

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions that terminated abnormally.

Collection Interval: 30 min

Peg Condition:

- Transaction times-out waiting for a response, and the maximum number of transmits has been reached.
- Transaction time-to-live limit is exceeded.
- Transaction terminated due to lack of resources.

Note: This measurement is NOT pegged for these conditions:

- Transaction involves an unknown service.
- Transaction involves an unregistered Routed Service.

Measurement Scope: Server

Recovery:

1. Check the ComAgent Exception report to further diagnose the reasons why transactions are failing.
2. Contact *My Oracle Support (MOS)* for assistance.

CATransEndAbnormRateAvg

Measurement ID: 9865

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 ID: 9866

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 ID: 9845

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions initiated by local User Layers that ended with an error response from a destination server.

Collection Interval: 30 min

Peg Condition: When a reliable response stack event (G=1, A=1, E=1) is received from a server to which a request was sent, and the response corresponds to a pending transaction record.

Measurement Scope: Server

Recovery:

No action necessary.

This measurement has value when compared against other measurements. Server applications may respond with errors as part of normal operations, as seen by ComAgent.

CATransEndErr

Measurement ID: 9846

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions initiated by local User Layers that ended abnormally with an error response from a destination server.

Collection Interval: 30 min

Peg Condition: When a valid reliable response stack event (G=1, A=0, E=1) is received from a server to which a request was sent, and the response corresponds to a pending transaction record.

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 *My Oracle Support (MOS)* for assistance.

CATransEndNoResources

Measurement ID: 9848

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions initiated by local User Layers that ended abnormally due to lack of resources.

Collection Interval: 30 min

Peg Condition: ComAgent receives a reliable request (G=1, R=1) from a local User Layer and ComAgent is unable to allocate resources to process the transaction.

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 *My Oracle Support (MOS)* for assistance.

CATransEndNoResponse

Measurement ID: 9847

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions initiated by local User Layers that ended abnormally due to a timeout waiting for a response.

Collection Interval: 30 min

Peg Condition: Limit on the number of retransmits is reached with no response and limit on the transaction time-to-live is exceeded.

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 *My Oracle Support (MOS)* for assistance.

CATransEndUnkwnSvc

Measurement ID: 9842

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to an unknown service.

Collection Interval: 30 min

Peg Condition: ComAgent receives a reliable request (G=1, R=1) from a local User Layer that refers to an unknown service.

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 *My Oracle Support (MOS)* for assistance.

CATransEndUnregSvc

Measurement ID: 9861

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of reliable transactions initiated by local User Layers that ended abnormally because they referred to a known service that lacked a registered User Layer.

Collection Interval: 30 min

Peg Condition: ComAgent receives a reliable request (G=1, R=1) from a local User Layer that refers to a known service that has no registered User Layer.

Measurement Scope: Server

Recovery:

A non-zero value in this measurement indicates a software malfunction.

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

CATransNoReTxMaxTTL

Measurement ID: 9895

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions abnormally ended because of Max Time to live exceeded without any retransmits.

Collection Interval: 30 min

Peg Condition: Maximum Time To Live period exceeded with no retransmission attempts and no response received for the transaction.

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 *My Oracle Support (MOS)* if assistance is needed

CATransRetx

Measurement ID: 9831

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of times stack events were retransmitted.

Collection Interval: 30 min

Peg Condition: ComAgent reliable transaction retransmit timer expires and the limit on the number of retransmits has not been reached.

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 *My Oracle Support (MOS)* for assistance.

CATransReTxExceeded

Measurement ID: 9894

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions abnormally ended because of Max number of Retries exceeded.

Collection Interval: 30 min

Peg Condition: Number of retransmits limit is reached with no response received for the transaction.

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 *My Oracle Support (MOS)* if assistance is needed

CATransStaleSuccessRsp

Measurement ID: 9862

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of times that a success response was received from an unexpected server and was accepted to end a transaction.

Collection Interval: 30 min

Peg Condition: ComAgent receives a success response stack event (G=1, A=1, E=1) that has a correlation ID for an existing pending transaction record but that is originated from a different server than to which the request was last sent.

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 *My Oracle Support (MOS)* for assistance.

CATransTTLExceeded

Measurement ID: 9893

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of reliable transactions abnormally ended because of Max Time to live exceeded.

Collection Interval: 30 min

Peg Condition: Maximum Time To Live period exceeded with at least one retransmission attempted and no response received for the transaction.

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 *My Oracle Support (MOS)* if assistance is needed

CATxDscrdBundle

Measurement ID: 9993

Measurement Group: ComAgent Exception

Measurement Dimension: Single

Measurement Type: Simple

Description: Number of egress bundled event discarded during routing.

Peg Condition: Each time an egress bundled event is discarded during routing

Collection Interval: 30 min

Measurement Scope: Site

Recovery:

No action required

CATxDscrdConnUnAvail

Measurement ID: 9802

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events discarded because connection was not in-service(down/blocked/not aligned).

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent that is discarded by ComAgent Stack, due to connection status not being in-service.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data egress messages are discarded by ComAgent due to connection unavailability reasons.

CATxDscrdDestUserIncmpat

Measurement ID: 9803

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events discarded because the remote doesn't support requested capabilities (either it doesn't support stack or event library or event library version is incompatible).

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent that is discarded by Communication Agent Stack, due to incompatibility in requested library id/version and the one known by Communication Agent.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data egress messages are discarded by Communication Agent due to remote not supporting requested capabilities.

CATxDscrdEncodeFail

Measurement ID: 9804

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events discarded because of serialization failures.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent that is discarded by Communication Agent Stack, due to any local encode failures.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data egress messages are discarded by Communication Agent due to local encode failure.

CATxDscrdInternalErr

Measurement ID: 9817

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of egress events discarded because of other unexpected internal processing error.

Collection Interval: 30 min

Peg Condition: For each egress StackEvent that is discarded by ComAgent Stack, due to internal processing errors for conditions not covered by other meas-pegs.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many egress messages are discarded by ComAgent due to internal software processing errors for conditions not covered by other measurement pegs.

CATxDscrdMxSendFail

Measurement ID: 9805

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of User Data egress events discarded because of failure reported by MxEndpoint.

Collection Interval: 30 min

Peg Condition: For each User Data egress StackEvent that is discarded by Communication Agent Stack, due to send failure as indicated by underlying transport.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many User Data egress messages are discarded by Communication Agent due to transport reported error condition.

CATxDscrdUnknownSvc

Measurement ID: 9849

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of non-reliable and non-request (G=0 or R=0) egress stack events discarded because they refer to an unknown service.This measurement indicates that ComAgent is improperly configured to support a local application.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent a non-reliable or non-request (G=0 or R=0) egress stack event that refers to an unknown service.

Measurement Scope: Server

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Configuration** > **Routed Services** screen to verify that all Routed Services expected by local applications are properly configured.
2. Contact *My Oracle Support (MOS)* for assistance.

CATxDscrdUnkServer

Measurement ID: 9819

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Single

Description: Number of egress events discarded because the destination server was unknown/not configured.

Collection Interval: 30 min

Peg Condition: For each egress StackEvent that is discarded by ComAgent Stack, due to unknown destination ip address contents in StackEvent.

Measurement Scope: NE, Server

Recovery:

No action required.

This value provides a measure of how many egress messages are discarded by ComAgent due to unknown destination ip address in StackEvent.

CATxDscrdUnregSvc

Measurement ID: 9860

Measurement Group: ComAgent Exception

Measurement Type: Simple

Measurement Dimension: Arrayed (by Service ID)

Description: Number of egress stack events discarded because they reference a known service that has no registered User Layer.

Collection Interval: 30 min

Peg Condition: User Layer submits to ComAgent an egress stack event that refers to a known service that lacks a registered User Layer.

Measurement Scope: Server

Recovery:

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 *My Oracle Support (MOS)* for assistance.

OAM.ALARM measurements

Table 27: OAM Alarm measurements

Measurement Tag	Description	Collection Interval
Alarm.Crit	The number of critical alarms.	5 minutes
Alarm.Major	The number of major alarms.	5 minutes

Measurement Tag	Description	Collection Interval
Alarm.Minor	The number of minor alarms	5 minutes
Alarm.State	The alarm state.	5 minutes

OAM.SYSTEM measurements

Table 28: OAM System measurements

Measurement Tag	Description	Collection Interval
System.CPU_UtilPct_Average	The average CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System.CPU_UtilPct_Peak	The peak CPU usage from 0 to 100% (100% indicates that all cores are completely busy).	5 minutes
System.Disk_UtilPct_Average	The average disk usage for the partition on which the COMCOL database resides.	5 minutes
System.Disk_UtilPct_Peak	The peak disk usage for the partition on which the COMCOL database resides.	5 minutes
System.RAM_UtilPct_Average	The average committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.	5 minutes
System.RAM_UtilPct_Peak	The peak committed RAM usage as a percentage of the total physical RAM. This measurement is based on the Committed_AS measurement from Linux/proc/meminfo. This measurement can exceed 100% if the kernel has committed more resources than provided by physical RAM, in which case, swapping will occur.	5 minutes

Measurement Tag	Description	Collection Interval
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

B

BIOS	Basic Input-Output System Firmware on the CPU blade that is executed prior to executing an OS.

C

CAPM	Computer-aided policy making
Charging Proxy Application	A DSR Application that is responsible for sending and receiving Diameter accounting messages.
CMOS	Complementary Metal Oxide Semiconductor CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.
ComAgent	Communication Agent A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.
Communication Agent	See ComAgent.
CPA	Capability Point Code ANSI

C

Charging Proxy Application - The Charging Proxy Application (CPA) feature defines a DSR-based Charging Proxy Function (CPF) between the CTFs and the CDFs. The types of CTF include GGSN, PGW, SGW, HSGW, and CSCF/TAS.

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

DB

Database

Data bus

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.

DSR

Data Set Ready

Diameter Signaling Router

A set of co-located Message Processors which share common

D

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

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

GLA

Gateway Location Application A DSR Application that provides a Diameter interface to subscriber data stored in the DSR's Policy Session Binding Repository (pSBR). Subscriber data concerning binding 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.

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

G

	than being limited to character based commands.

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

I

IMSI	International Mobile Subscriber Identity A unique internal network ID identifying a mobile subscriber. International Mobile Station Identity
IPFE	IP Front End A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

K

KPI	Key Performance Indicator

M

MP	Measurement Platform Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing.

M

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. 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

NAI

Nature of Address Indicator

Standard method of identifying users who request access to a network.

Network Access Identifier

The user identity submitted by the client during network authentication.

NPA

Number Plan Area

The North American “Area Codes.” (3 digits: 2- to-9, 0-or 1, 0-to-9. Middle digit to expand soon).

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.

R

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

S

S

SBR	Subsystem Backup Routing Session Binding Repository - A highly available, distributed database for storing Diameter session binding data
SDS	Subscriber Database Server Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.
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

S

SOAP	Simple Object Access Protocol
SW	Software