Oracle® Tuxedo System and Applications Monitor Plus

User's Guide

Release 22c
F96913-03
July 2026

Oracle Tuxedo System and Applications Monitor Plus User's Guide, Release 22c

F96913-03

Primary Authors: Preeti Gandhe, Priya Pathak

Contributing Authors: Tulika Das

Contributors: Maggie Li

Contents

1 Using Oracle TSAM Plus Console

1.1 Overview 1
1.1.1 User Accessibility 1
1.1.2 Top Menu Bar 2
1.1.3 Component Tree 2
1.1.3.1 Tuxedo Domains Component Tree 2
1.1.3.2 CICS Regions Component Tree 3
1.1.3.3 Batch Systems Component Tree 3
1.1.3.4 IMS Systems Component Tree 3
1.1.4 Search Panel 6
1.1.5 Domains Dashboard 6
1.1.5.1 Viewing Domain Group Dashboard 7
1.1.5.2 Viewing Individual Domain Dashboard 8
1.1.5.3 Customizing a Dashboard 8
1.2 Using Oracle TSAM Plus Console 10
1.2.1 Monitoring Policy 10
1.2.1.1 Tuxedo Monitoring Policy 10
1.2.1.2 CICS Runtime Monitoring Policy 18
1.2.1.3 IMS Runtime Monitoring Policy 21
1.2.2 Tuxedo Metrics Monitoring 23
1.2.2.1 Call Path 23
1.2.2.2 Call Pattern 32
1.2.2.3 Service 34
1.2.2.4 XA Transaction 36
1.2.2.5 Domain Gateway 38
1.2.2.6 BRIDGE 39
1.2.2.7 GWWS 40
1.2.3 CICS/IMS/Batch Runtime Metrics Monitoring 41
1.2.3.1 CICS Transactions 41
1.2.3.2 CICS Terminals 42
1.2.3.3 Batch Jobs 43
1.2.3.4 IMS Transactions 45
1.2.3.5 IMS Programs 45

1.2.3.6 IMS System Traces 46
1.2.4 CICS/IMS/Batch Management 48
1.2.4.1 Batch Jobs Submit 48
1.2.4.2 Batch Jobs Search/Display 49
1.2.4.3 Batch Syslog Search/Display 52
1.2.4.4 CICS Resources View/Edit 53
1.2.4.5 IMS Resources View/Edit 53
1.2.5 User/Data Management 54
1.2.5.1 User Management 54
1.2.5.2 Data Management 57
1.2.5.3 Global Parameters 58
1.2.5.4 Blackout 61
1.2.5.5 Domain Group Management 63
1.2.6 Load Generator 64
1.2.7 Alert Monitoring 64
1.2.7.1 Tuxedo Alert Definition 65
1.2.7.2 CICS Alert Definition 68
1.2.7.3 IMS Alert Definition 70
1.2.7.4 Batch Alert Definition 72
1.2.7.5 Alert Query 75
1.2.7.6 System Alerts Supported 78
1.2.7.7 Alert Metrics Tables 78
1.3 Oracle TSAM Plus Group/User Privileges 81
1.4 AI Operations Assistant 82
1.4.1 Overview 82
1.4.2 AI Setup Prerequisites 82
1.4.3 Features of the TSAM Operations Assistant 82
1.4.4 Accessing the TSAM Operations Assistant 83
1.4.5 Using the Operations Assistant 83
1.4.6 Configuring the Operations Assistant 84
1.4.7 Sample Questions 85

2 Oracle Tuxedo Scripting Tool

2.1 Using the Tuxedo Scripting Tool 1
2.1.1 What is the Tuxedo Scripting Tool? 1
2.1.1.1 How Does TXST Work? 1
2.1.2 Modes of Operation 2
2.1.2.1 Interactive Mode 2
2.1.2.2 Script Mode 2
2.1.2.3 Embedded Mode 2
2.1.3 Main Steps for Using TXST 3

2.1.3.1 Setting Up Your Environment 3
2.1.3.2 Invoking TXST 3
2.1.3.3 Requirements for Entering TXST Commands 4
2.1.3.4 Running Scripts 4
2.1.3.5 Exiting TXST 6
2.1.3.6 Getting Help 6
2.1.3.7 Recording User Interactions 7
2.1.3.8 Redirecting TXST Output to a File 7
2.2 Navigating MBeans 7
2.2.1 Navigating and Interrogating Mbeans 7
2.2.1.1 Changing the Current Management Object 8
2.2.1.2 Navigating and Displaying Configuration MBeans Example 8
2.2.2 Browsing Runtime MBeans 10
2.2.3 Finding MBeans 10
2.3 Managing the Server Life Cycle 11
2.3.1 Starting and Stopping 11
2.3.1.1 Domain 11
2.3.1.2 Machine, Group, and Server 11
2.3.2 Suspending and Resuming 11

3 TSAM Plus Accounting and Chargeback

3.1 Accounting Information Output 1
3.1.1 Prerequisite 1
3.1.2 Configuration 1
3.1.3 Samples 3
3.2 Accounting Information Analyzing 3
3.2.1 Configuration 3
3.2.2 Output 5
3.2.3 Samples 5
3.2.3.1 Sample 1 - Default Usage 5
3.2.3.2 Sample 2 5
3.2.3.3 Sample 3 6
3.3 Known Issues 6

4 User Payload Collection

4.1 Overview 1
4.2 Supported User Payload Buffer Types 1
4.3 Determine User Payload Storage 1
4.3.1 User Payload Record in Oracle Database 2
4.3.2 User Payload Record in Hadoop 2

4.3.2.1 File Naming 3
4.3.2.2 Content Format 3
4.3.3 User Payload Record in Local File 4
4.3.4 Specifying User Payload Storage from TSAM Plus Console 4
4.4 Configuring User Payload Collection 4
4.4.1 Defining Payload Collection Data Criteria 5
4.4.2 Defining Payload Collection Result Filter 6
4.5 Exporting Collected User Payload Data 7
4.5.1 APIs for Data Export 7
4.5.1.1 PayloadRepository 8
4.5.1.2 FilePayloadIterator 8
4.5.1.3 FilePayloadRepository 9
4.5.1.4 HadoopPayloadIterator 10
4.5.1.5 HadoopPayloadRepository 11
4.5.1.6 payloaddump 13
4.5.1.7 PayloadRecord 14
4.5.1.8 PayloadValue 16
4.5.1.9 TSAMDBPayloadIterator 19
4.5.1.10 TSAMDBPayloadRepository 20
4.5.1.11 Enum PayloadType 22
4.5.1.12 Payload API Samples 23
4.5.2 Payload Dump Tool 24

5 Using Test Load Generator

5.1 Overview 1
5.2 Creating Call Path Policy for a Replay 1
5.3 Creating a Replay Definition 1
5.3.1 Setting Replay Definition Attributes 2
5.4 Running a Replay 2
5.4.1 Execution Plan File 3
5.4.1.1 Normal Mode Attributes 3
5.4.1.2 Stress Test Mode Attributes 4
5.4.2 Replay Security Profile 5
5.4.3 Replay Execution Result 5
5.5 Running a Replay in Auto-Created Test Domain 6
5.5.1 Configuration File 6
5.5.2 Executing tlgdomgen.py 7

A Examples of Questions Users Can Ask Through the Operations Assistant

A.1 Product Overview and Release Information A-1

A.2 Getting Started to Use TSAM Plus A-1
A.3 Capacity, Scaling, and Data Management A-2
A.4 Monitoring Configuration and Policies A-2
A.5 Dashboard, Performance, and Health A-2
A.6 Troubleshooting and Logs A-2
A.7 Security A-3
A.8 Alerts A-3
A.9 Domain, Group, Server, and Service Queries A-3
A.10 Call Path, Transaction, Payload, and Runtime Queries A-4

List of Examples

2-1 Changing the Current Management Object 8

2-2 Navigating and Displaying Configuration MBeans 8

2-3 Finding MBeans 10

4-1 API Sample 1 23

4-2 Payload API Sample 2 24

List of Tables

1-1	IMS System Summary Table	4
1-2	MPP Region Details	4
1-3	IMS Region Summary	5
1-4	IMS Region Details	6
1-5	Metrics Chart Parameters	9
1-6	Button Bar	11
1-7	Call Path Tab Options	13
1-8	Service Tab Options	16
1-9	XA Transaction Tab Options	16
1-10	Domain Gateway Tab	17
1-11	Sub Controls of BRIDGE Panel	18
1-12	GWWS Panel Tab Options	18
1-13	Monitoring Policy List Button Bar	19
1-14	CICS Transaction Tab Options	20
1-15	CICS Terminals Tab Options	20
1-16	Button Bar	21
1-17	IMS Transaction Tab Options	22
1-18	IMS Program Tab Options	23
1-19	Call Path Query By Filter Options	24
1-20	Call Path Results List Panel Options	27
1-21	Call Path Details Panel Options	30
1-22	Call Pattern Filter Panel Options	32
1-23	Call Pattern Results List Panel Options	33
1-24	Call Pattern Details Panel	34
1-25	Service Selection Options	34
1-26	Service Monitoring Results Panel Options	36
1-27	XA Transaction Query by Scope Panel Options	37
1-28	XA Transaction Results List Panel Options	37
1-29	XA Transaction Detail Panel Options	38
1-30	Domain Gateway Selection Panel Options	39
1-31	Domain Gateway Monitoring Panel Options	39
1-32	GWWS Query by Filter Panel Options	40
1-33	GWWS Live/History Monitoring Panel Options	41
1-34	CICS Transactions Query By Filter Options	42
1-35	CICS Transactions Live/History Monitoring Options	42
1-36	CICS Terminals Query By Filter Options	43

1-37	CICS Terminals Live/History Monitoring Graph Options	43
1-38	JES Metrics Query by Filter Panel	44
1-39	JES Monitor View	44
1-40	IMS Transaction Query By Filter Options	45
1-41	IMS Transaction Live/History Monitoring Options	45
1-42	IMS Program Query By Filter Options	46
1-43	IMS Transaction Live/History Monitoring Options	46
1-44	Query Filters	47
1-45	Detailed Information	47
1-46	Job File Information List Panel Options	49
1-47	JES Jobs Query By Filter Options	50
1-48	Jobs Query Results List	50
1-49	JES Syslogs Query by Filter Options	52
1-50	User List Menu Bar Options	55
1-51	Group List Button Bar Options	56
1-52	TSAM Plus Global Properties	59
1-53	Manager Parameter Properties	60
1-54	Blackout List Table Content	61
1-55	Blackout List Table Controls	62
1-56	Create/Edit Blackout Fields	62
1-57	Domain Group List	64
1-58	Tuxedo Alert Definition Menu Bar Options	65
1-59	Tuxedo Alert Columns	65
1-60	Alert Properties Options	66
1-61	CICS Alert Definition List Menu Bar	68
1-62	Alert Definition List Columns	69
1-63	Alert Properties Options	69
1-64	IMS Alert Definition List Menu Bar	71
1-65	Alert Definition List Columns	71
1-66	Alert Properties Options	72
1-67	Batch Alert Definition List Menu Bar	73
1-68	Alert Properties Options	73
1-69	Batch Alert By Filter Options	74
1-70	JES Job Type Detailed Information	74
1-71	JES Metrics Type Detailed Metrics	74
1-72	Alert Query Filtering Conditions	75
1-73	Alert Query Columns	76

1-74	Historical Alerts Query Conditions Options	77
1-75	System Alerts Supported	78
1-76	Call Path Alert Metrics Table	78
1-77	Service Alert Metrics Table	79
1-78	GWTDOMAIN/BRIDGE Alert Metrics Table	79
1-79	GWWS Alert Metrics Table	79
1-80	XA Transaction Alert Metrics Table	79
1-81	CICS Transaction Alert Metrics Table	80
1-82	CICS Terminals Alert Metrics Table	80
1-83	IMS Transaction Alert Metrics Table	80
1-84	IMS Program Alert Metrics Table	80
1-85	Oracle TSAM Plus Group/User Privileges	81
2-1	Ant Task Attributes	6
2-2	Details about targets	11
4-1	Supported Oracle Tuxedo Buffer Types in User Payload	1
4-2	User Payload Data in MON_PAYLOAD	2
4-3	Data Criteria Table	5
4-4	APIs for Data Export	7
5-1	Replay Definition Attributes	2
5-2	Replay Definition Service Calls Attributes	2
5-3	Replay Agent Parameters	3
5-4	General Attribute	3
5-5	Normal Mode Attributes	3
5-6	Stress Test Mode Attributes	5
5-7	Configuration File Parameters	6

1

Using Oracle TSAM Plus Console

This chapter contains the following topics:

- Overview
- Using Oracle TSAM Plus Console
- Oracle TSAM Plus Group/User Privileges
- AI Operations Assistant

1.1 Overview

The Oracle TSAM Plus monitoring console allows you to specify the Oracle Tuxedo components you want to monitor, as well as track events and alerts.

> **Note**
>
> To get the best experience and full functionality of Oracle TSAM Plus Console, Oracle recommends you use the following Web browsers.
>
> - Firefox 146.0.1
> - Google Chrome 143.0

The Oracle TSAM Plus Console has the following major sections:

- User Accessibility
- Top Menu Bar
- Component Tree
- Search Panel
- Domains Dashboard

1.1.1 User Accessibility

User accessibility settings can be adjusted from the log-in screen and the console page.

- Log-in Screen
  In the upper left-hand corner of the log-in screen, click the **Settings** drop-down menu. You can select the following three options; the settings take effect immediately:
  - I use a screen reader
    Accessibility-specific constructs are added to improve screen reader behavior.
  - I use high contrast colors
    Application display uses high-contrast instead of the default contrast.
  - I use large fonts
    Application display uses large fonts instead of the default size fonts.

- Console Page
  In the upper right-hand corner of the Oracle TSAM Plus Console page, click **Accessibility**; the **Accessibility Preferences** page appears. It has the same three user accessibility options as the log-in screen.

  When you have selected your options, click **OK**; the settings take effect immediately.

1.1.2 Top Menu Bar

The top menu bar contains the following Oracle TSAM Plus monitoring console functionality:

Policy: Define and manage system policies.

Tuxedo Metrics: Query Oracle Tuxedo monitoring metrics.

CICS/IMS/Batch Runtime Metrics: Query Oracle Tuxedo Application Runtime monitoring metrics.

CICS/IMS/Batch Management: View/edit CICS/IMS resources, submit/query batch jobs and search bath syslog.

Alert: Define and query alerts.

Load Generator: Create the replay definition from call paths.

Management: Define user management, data management, global parameter settings, and blackout.

Help: On-line help page.

1.1.3 Component Tree

- Tuxedo Domains Component Tree
- CICS Regions Component Tree
- Batch Systems Component Tree
- IMS Systems Component Tree

1.1.3.1 Tuxedo Domains Component Tree

Tuxedo Domains tree displays the Tuxedo Domain Group -> Domain -> Machine -> Group -> Server -> Service hierarchy information.

All service nodes are hidden in the Tuxedo Component Tree by default. You can click **Show Service** to display them. You can click **Verbose View** to show more information.

By default, the component tree displays the first domain. You can specify the domain to be displayed in the component tree from the Domain list. Your preference is remembered until the selected domain does not exist anymore.

The domain structure in the component tree and relevant pages will not automatically change after you logged in. Click **Refresh** to display the current domain structure.

In the component tree, different icon colors indicate different nodes status:

- Green: the domain and all its components are active
- Yellow: at least one child node under current node is in inactive or unhealthy status
- Red: the domain or component is inactive

Particularly, if an alert icon arises, it indicators the domain contains unread alerts.

You can filter the component tree to display only domains with unread alerts or inactive components, domains in particular group, or particular domain using the **Domain** list.

You can view the overall status for all domains, a Tuxedo domain group, or a Tuxedo domain by clicking corresponding node in the component tree. For more information, see Domains Dashboard.

1.1.3.2 CICS Regions Component Tree

CICS Regions tree displays the CICS Region -> CICS Transaction/CICS Terminals hierarchy information.

Besides hierarchy information, other information is displayed (such as Oracle Tuxedo version, Domain model, server status, etc.). Certain tasks (for example, Create Policy) can be performed directly on the tree nodes.

1.1.3.3 Batch Systems Component Tree

Batch Systems tree displays the JES application -> JES nodes -> Tuxedo JES servers hierarchy information.

> **Note**
>
> Similar to the `artjesadmin changeconcurrent` command, the maximum concurrent job number can also be changed in TSAM Plus console. Right click **ARTJESINITIATOR** in the JES component tree, there is an menu item named **Change Concurrent Jobs**. If the server is active, the menu item is available. On this option is selected, a pop-up window appears with the current max concurrent job number displayed. Input a number between 1 and 32767, the concurrent job number is modified.

1.1.3.4 IMS Systems Component Tree

IMS Systems tree displays the IMS systems ->Tuxedo Domain ->Transactions/Programs hierarchy information.

- IMS System Summary
- IMS System Summary Table
- IMS System Details Panel
- IMS Region Summary
- IMS Region Summary Table
- IMS Region Details Panel

1.1.3.4.1 IMS System Summary

In the IMS Systems tree, you can right-click the root node and select **Summary** to view the system summary page.

The ART IMS system summary page contains two panels.

1.1.3.4.2 IMS System Summary Table

The system summary table lists all the ART IMS systems (domains) currently monitored by TSAM Plus.

The following table describes each column:

Table 1-1 IMS System Summary Table

Column Name	Description
Sysman Name	IMS system name. It is the first part string in the domain ID before the first ":" character. You can click the system name to go to the corresponding ART IMS Region Summary page.
Machine Names	The comma-separated list of all machine names in the domain.
Status	Domain status, Active or Inactive.
Last Start Time	The last startup time of the domain.
Number of Machines	Machine number in the domain.

1.1.3.4.3 IMS System Details Panel

When you select an IMS system line in the Summary table, the related system information is displayed in the Details panel below. The three tabs, MPP, BMP, and BMPT, represent three types of the ART IMS region monitored by TSAM Plus. The information shown for each region type are very similar. The following table describes the MPP region type details.

Table 1-2 MPP Region Details

Metrics		Description
Number of MPP Regions		The total number of MPP regions (ARTIMPP processes) in the domain.
Totals Since Startup	CPU Consumption	Total CPU consumption. The system and user CPU of all transactions since the system startup.
	System CPU	Total system CPU consumption of all transactions since the system startup.
	User CPU	Total user CPU consumption of all transactions since the system startup.
	Transaction Count	Total transaction count since the system startup.
Totals Since Last Hour	CPU Consumption	Total CPU consumption. The system and user CPU of all transactions in the last hour.
	System CPU	Total system CPU consumption of all transactions in the last hour.
	User CPU	Total user CPU consumption of all transactions in the last hour.
	Transaction Count	Total transaction count in the last hour.
Averages in the Last Hour	Transaction Time	The average transaction elapse time in the last hour (total transaction time / transaction count).
	Transaction CPU Consumption	The average transaction CPU time in the last hour (system and user CPU).
	Transaction System CPU	The average transaction system CPU time in the last hour.

Table 1-2 (Cont.) MPP Region Details

Metrics		Description
	Transaction User CPU	The average transaction user CPU time in the last hour.
	Transaction Rate	The transaction count in each 15 minutes time window in the last hour.

1.1.3.4.4 IMS Region Summary

In the IMS Systems tree, you can right-click the domain node and select Summary to view the region summary page.

The ART IMS region summary page contains two panels.

1.1.3.4.5 IMS Region Summary Table

The IMS Region Summary table lists all the ART IMS regions (servers) currently monitored by TSAM Plus in this domain.

The following table describes each column:

Table 1-3 IMS Region Summary

Column Name	Description
Region	The region name is in the format of "`process name/group name/server id`"" for example, `ARTIMPP/GROUP1/6`. **Note** each UBB server entry is considered as one region, no matter what MIN and MAX values are configured. One region can actually contains multiple server instances.
Region Type	The region type is one of the following values: • BMP (Batch-oriented): The process is ARTIBMP • BMP (Transaction-oriented): The process is ARTIBMPT • IFP: IMS Fast Path Region. The process is ARTIMPP, and "-p" is not configured in the CLOPT of the server. • MPR: Message Processing Region. The process is ARTIMPP, and "-p" is configured in the CLOPT of the server.
Status	Tuxedo server status, Active or Inactive.
Number of Servers	The started server instances number.
Last Start Time	The last server start-up time.

1.1.3.4.6 IMS Region Details Panel

When you select an IMS region line in the Summary table, the related IMS region information is displayed in the Details panel below.

The following table describes the metrics shown in the main area.

Table 1-4 IMS Region Details

Metrics		Description
Totals Since Startup	CPU Consumption	Total CPU consumption. The system and user CPU of all transactions in this region since the server startup.
	System CPU	Total system CPU consumption of all transactions in this region since the server startup.
	User CPU	Total user CPU consumption of all transactions in this region since the server startup.
	Transaction Count	Total transaction count in this region since the server startup.
Totals Since Last Hour	CPU Consumption	Total CPU consumption, system + user CPU of all transactions in this region in the last hour.
	System CPU	Total system CPU consumption of all transactions in this region in the last hour.
	User CPU	Total user CPU consumption of all transactions in this region in the last hour.
	Transaction Count	Total transaction count in this region in the last hour.
Averages in the Last Hour	Transaction Time	The average transaction elapse time in the last hour (total transaction time / transaction count).
	Transaction CPU Consumption	The average transaction CPU time in the last hour (system and user CPU).
	Transaction System CPU	The average transaction system CPU time in the last hour.
	Transaction User CPU	The average transaction user CPU time in the last hour.
	Transaction Rate	The transaction count in each 15 minutes time window in the last hour.c

1.1.4 Search Panel

Search component tree elements.

1.1.5 Domains Dashboard

When you log into Oracle TSAM Plus monitoring console, the Domains Dashboard is displayed with overall Tuxedo domains and domain groups metrics. It presents the following information:

- Severity-level unread alert count. To read the alerts of a severity level, click the number after the level.
- An aggregated view of all domains components availability. When clicking the inactive (red) part of a pie chart, a window is popped up showing all the inactive items in detail.
- All domains and domain groups metrics charts

The metrics charts show the related metrics data captured in the selected time range. When you move the cursor over a data node, the data value is shown up. For the metrics data collection interval, you can set it from the **Management-> Global Parameters** page. For more information, see Global Parameters.

The domains dashboard always displays the first three metrics charts positioned in individual domain or domain group dashboard for a quick glimpse. By default, these charts are displayed with the data for all services in last 24 hours.

- Throughput
  The number of Tuxedo service calls per minute.

- Response Time
  The average response time (in microseconds) of Tuxedo service calls.
- Failure Number
  The number of Tuxedo service call failures per minute

For the domain groups presented in the dashboard, you can manage them from the **Management -> Domain Group Management** page. For more information, refer to Domain Group Management.

From any domain or domain group dashboard, you can set the dashboard to refresh the data periodically by choosing the **Auto Refresh** box on the top and specifying the refresh interval from the list. The refresh interval you set affects all dashboard pages.

> **Note**
>
> This feature is only available when Oracle database is used, and is not available if you are using Derby database.

- Viewing Domain Group Dashboard
- Viewing Individual Domain Dashboard
- Customizing a Dashboard

1.1.5.1 Viewing Domain Group Dashboard

To view a domain group dashboard, click the domain group name in the dashboard or left component panel.

- Unread Alerts
  Displays severity-level unread alert count. To read the alerts of a severity level, click the number after the level.
- Availability
  Displays aggregated availability of all domains belonging to the group. When clicking the inactive (red) part of a pie chart, a window is popped up showing all the inactive items in detail.
- Availability
  Displays aggregated availability of all domains belonging to the group. When clicking the inactive (red) part of a pie chart, a window is popped up showing all the inactive items in detail.
- Metrics Charts
  The throughput, response time, and failure number charts are displayed with the data in last 24 hours by default. For any metrics chart, you can change the time range to show the chartfrom the drop-down list.

  If you have set the chart to show metrics per service, you get multiple lines on the chart representing each selected service in different colors. You can hide or unhide certain services lines by checking or unchecking the short bar (-) icon before the desired services name under the chart.

You can also customize the charts in dashboard. For more information, refer to Customizing a Dashboard.

Click the group name on the top of the dashboard, you enter the domain group details page that presents the availability and the first three metrics charts of the domain group for each

individual member domain. You can sort the domain list in ascending or descending order by the metrics selected in the **Order By** list.

To go further to view and edit individual domain dashboard, click the domain name. For more information, refer to Viewing Individual Domain Dashboard.

1.1.5.2 Viewing Individual Domain Dashboard

To view individual domain dashboard, click the domain name in any dashboard or left component panel.

- Service Statistics
  Click this link to enter the Service Statistics page, which shows you the last-time collected metrics data breakdown for each services.

  You can filter the list to display desired services. Type the name keywords (case-insensitive) in the Filter textbox and click the button. You can input mulitiple keywords separated by commas, semicolons, or spaces.

  You can also export the service statistics table as a CVS file by clicking **Export to CVS**.

  To view detailed metrics data collected for a service, right-click the service row and select one of the time range:

  – 24 Hours: displays the aggreated data of every collection interval in 24 hours.
  – 7 Days: displays the aggreated data for every hour in the past six days
  – 31 Days: displays the aggreated data for every day in the past month.
- Unread Alerts
  Displays severity-level unread alert count. To read the alerts of a severity level, click the number after the level.
- Availability
  Displays availability of servers in the domain. When clicking the inactive (red) part of a pie chart, a window is popped up showing all the inactive items in detail.
- Metrics Charts
  The throughput, response time, and failure number charts are displayed with the data in last 24 hours by default. For any metrics chart, you can change the time range to show the chart from the drop-down list.

  If you have set the chart to show metrics per service, you get multiple lines on the chart representing each selected service in different colors. You can hide or unhide certain services lines by checking or unchecking the short bar (-) icon before the desired services name under the chart.
  You can also personalize the charts in dashboard. For more information, refer to Customizing a Dashboard.

1.1.5.3 Customizing a Dashboard

In a domain group or domain dashboard, you can chart metrics over any time period you choose, create your own charts to suit your need, and define the key services for regular monitoring. Click the **Customize** button in the upper right page to activate customization mode.

> **Note**
>
> Any customization configuration made in the group dashboard does not affect the underlying domain dashboard definition and vice versa.

- Defining Key Services
- Editing a Metrics Chart
- Adding a Metrics Chart
- Moving or Removing a Panel

1.1.5.3.1 Defining Key Services

In many cases, you may want to monitor a fixed set of services regularly. You just need to define them as key services to avoid repeatedly specifying target services. The key services can then be used when you edit or create a chart.

To define the key services for a domain, click the **Key Services** in the upper right of the domain dashboard page and add the desired services to the left box.

To define the key services for a group, refer to Domain Group Management.

1.1.5.3.2 Editing a Metrics Chart

To customize the chart that appears, click **Edit** in any metrics chart field and define the parameters listed in the following table.

Table 1-5 Metrics Chart Parameters

Options	Description
Chart Name	Specifies a name to identify the chart.
Service List	Specifies the services you want to monitor on the chart: • All Services • Key Services: The key services you defined before for regular monitoring purpose. For more information, refer to Defining Key Services. • Select Manually: Select particular services you want to monitor in the list.
Metrics	Specifies the metric chart type: • Throughput (per minute): Number of Tuxedo service calls per minute • Number of Successes (per minute): Number of success Tuxedo service calls per minute • Number of failures (per minute): Number of failed Tuxedo service calls per minute • Number of System Failures (per minute): Number of Tuxedo service calls with system failure per minute • Number of User Failures (per minute): Number of Tuxedo service calls with user failure per minute • Response Time (microsecond): Average Tuxedo service call response time • Wait Time (microsecond): Average Tuxedo service call wait time • Execution Time (microsecond): Average Tuxedo service execution time • CPU Time (microsecond): Average Tuxedo service CPU consumption time
Range	Specifies the time range to present the data on the chart. You can choose to display the data in: • Last Hour: the aggregation interval is every metrics collection interval • Last 24 Hour: the aggregation interval is every metrics collection interval • Last Week: the aggregation interval is one hour • Last 31 Day: the aggregation interval is one day By default, the chart presents data in last 24 hours.
Per Service	This option is available when is not set to **All Service**. When selected, the chart shows lines of each service separately in different colors.
Chart Type	Specifies the chart type: Line, Bar, Area, Combination, or Line with Area.
Chart Size	Specifies the width of the chart.

1.1.5.3.3 Adding a Metrics Chart

You can create up to 12 new charts by clicking **Add** in the upper right page. For descriptions of parameters in the window that appears, refer to Metrics Chart Parameters.

1.1.5.3.4 Moving or Removing a Panel

You can move up, move down, or delete any chart by clicking related function buttons at the top of the chart field.

Only the top three charts positioned in an individual domain dashboard are presented in the group or all domains dashboard.

1.2 Using Oracle TSAM Plus Console

This section contains the following topics:

- Monitoring Policy
- Tuxedo Metrics Monitoring
- CICS/IMS/Batch Runtime Metrics Monitoring
- CICS/IMS/Batch Management
- User/Data Management
- Load Generator
- Alert Monitoring

1.2.1 Monitoring Policy

Oracle TSAM Plus provides comprehensive monitoring control of Oracle Tuxedo infrastructure behavior. Policy Management allows you to do the following:

- Organize monitoring requirements into significant and useful monitoring policy solutions.
- Manage monitoring policy (including import, export and usage tracking)
- Define monitoring policy entries for Oracle Tuxedo components and dynamic conditions
- Selectively enable and disable real-time communication with monitored Oracle Tuxedo back-end components.

This section contains the following topics:

- Tuxedo Monitoring Policy
- CICS Runtime Monitoring Policy
- IMS Runtime Monitoring Policy

1.2.1.1 Tuxedo Monitoring Policy

On the menu bar, click **Policy** and select **Tuxedo Monitoring Policy** from the drop-down menu; the **Monitoring Policy List** page appears. It displays the existing defined policies and allows you to view, add, edit, or delete policies. This section contains the following topics:

- Monitoring Policy List Page
- Create/Edit Policy Page

1.2.1.1.1 Monitoring Policy List Page

The Monitoring Policy List page allows you to create and manage the Oracle Tuxedo component monitoring policies.

- Button Bar
- Policy List Table
- Policy for PeopleSoft Domains

1.2.1.1.1.1 Button Bar

The following table lists the Monitoring Policy List button bar functions:

Table 1-6 Button Bar

Button	Description
View	From the drop-down menu, select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Add	Creates a new monitor policy. The maximum policy name character length is 255. **Note** You can also add a new policy by right-clicking a Domain listed in the Oracle Tuxedo Components panel.
Delete	Deletes selected monitoring policies.
Enable	Enables selected monitoring policies.
Disable	Disables selected monitoring policies.
Edit	Edits selected monitoring policies.
Clone	Clones a new policy from a selected policy.
Import	Imports previously exported policies from a user-specified location.
Export	Exports selected policies in an file to a user-specified location.
Refresh	Updates the policies displayed in the Policy List table.

1.2.1.1.1.2 Policy List Table

The Policy List table displays the following columns:

- **Select:** Allows you to select all or individual policies
- **Name:** Displays the current policy names.
- **Status**: Displays the policy status.
  - **enabled**: The corresponding request is sent to Oracle Tuxedo.
  - **disabled**: The corresponding request is not sent to Oracle Tuxedo.

> **Note**
>
> Policy monitoring does not take effect until the impacted Oracle Tuxedo processes have started.

- **Domain ID**: Displays the domain identifier attached to the policy as follows: `DOMAINID:Master:IPCKEY`
- **Tuxedo Components:** String that represents policy impact scope of Tuxedo resources in selected domain. It is FML32 boolean expression compliant. For example: (`TA_PMID%%'.*BOXBANK*'`) indicates using an FML32 boolean expression for machine selection.

1.2.1.1.1.3 Policy for PeopleSoft Domains

TSAM Plus provides out-to-box policies for monitoring Oracle PeopleSoft Applications. The PeopleSoft domain is displayed different from common Tuxedo domains in the list. Its Domain ID is separated by three colons, for example `APPDOM_217989:LOCALHOST.COM:PS_DOMAI:PS`. To monitor PeopleSoft domains, select the policy and click **Enable**.

1.2.1.1.2 Create/Edit Policy Page

The Create/Edit Policy page contains the following sections:

- Tuxedo Component Panel
- Monitoring Policy Panel
- Call Path Tab
- Service Tab
- XA Transaction Tab
- Domain Gateway Tab
- BRIDGE Tab
- GWWS Tab

1.2.1.1.2.1 Tuxedo Component Panel

The Tuxedo Component panel contains the following selections:

- **Domain**: Required.
- **Machine**: Optional.
- **Group**: Optional.
- **Server**: Optional.

Machine, Group, and Server can also accept FML32 boolean expressions. Click the radio button to select an input method (from the drop-down list or manually enter an FML32 boolean expression). The value of each level is determined by its parent level (except for Domain).One monitoring policy must be specified for one domain.

1.2.1.1.2.2 Monitoring Policy Panel

The Monitoring Panel contains the following tabs:

Call Path Tab

Service Tab

XA Transaction Tab

Domain Gateway Tab

BRIDGE Tab

GWWS Tab

To use the listed tab options, click the **Enable** check box. If enable is not selected, all tab options are disabled. One monitoring policy can contain multiple monitoring categories.

1.2.1.1.2.3 Call Path Tab

The following table lists the **Call Path** tab options:

Table 1-7 Call Path Tab Options

Options	Description
Basic Policy Options	-
Enable	Enables/disables call path monitoring. **Note** The fist policy deployed to the Tuxedo domain takes effect when there are more than one policies enabled on a Tuxedo target. The fist policy attributes, such as extended, bridge decode, affect the whole call path.
Ratio/Interval	Selects Ratio or Interval policy. If multiple policies cover one initiator process and the ratio or interval policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. • Ratio: Accepts a value range of 1-65535. It indicates that monitoring starts for a certain number of requests. The default value is 1 (indicating each request is monitored). • Interval: Accepts a value range of 1-65535. It indicates a period of time (in seconds) that monitoring can be started. It is exclusive of ratio settings. The default value is 1. The ratio/interval control only applies to the call path initiator.
Alert Only	Specifies alert evaluation only. No metrics are sent to manager.
Bridge Decode	Allows all BRIDGEs in the call path to decode messages. By default, BRIDGEs do not decode messages and the call path representation does not show BRIDGE points. **Note** Use this option carefully. Decode/encode impacts application performance.

Table 1-7 (Cont.) Call Path Tab Options

Options	Description
Enable Extended Monitoring	When this option is enabled, the extended monitoring data reported by the tsambegin() and tsamend() API are collected by call path. These API are invoked automatically in Oracle Tuxedo ART for CICS and Batch when a CICS command, EXEC SQL, or IMS DLI is invoked. Following SQL are supported by OCI: **Note** To monitor Pro*C sql by OCI , OCI library must be loaded in TSAM Plus Agent. Specify `libclntsh.so` location in the lib path when starting up the domain Following SQL are supported by OCI: • `EXEC SQL ALTER` • `EXEC SQL AUDIT` • `EXEC SQL COMMENT` • `EXEC SQL CREATE` • `EXEC SQL DROP` • `EXEC SQL GRANT` • `EXEC SQL NOAUDIT` • `EXEC SQL RENAME` • `EXEC SQL REVOKE` • `EXEC SQL TRUNCATE` • `EXEC SQL DELETE` • `EXEC SQL EXPLAIN PLAN` • `EXEC SQL INSERT` • `EXEC SQL LOCK TABLE` • `EXEC SQL OPEN` • `EXEC SQL SELECT` • `EXEC SQL UPDATE` • `EXEC SQL SAVEPOINT` • `EXEC SQL EXECUTE` • `EXEC SQL PREPARE` • `EXEC SQL SET ROLE` • `EXEC SQL EXECUTE END-EXEC`
Enable Extended Monitoring Limit	When this option is enabled, it specifies the maximum extended call path segments that can be generated in a call path when "Enable Extended Monitoring" is enabled. The acceptable value range is 1~ 2147483647. Default value is 1000.
Enable Service Contract Discovery	When this option is selected, the monitored services contract information is collected. For more information, see User Payload Collection.
Define Payload Collection	Click this button to specify the payload collection policies. For more information, see User Payload Collection.
Define Alert	Displays the alert definition page. For more information, see Tuxedo Alert Definition.

Table 1-7 (Cont.) Call Path Tab Options

Options	Description
Define Conditional Filter	Click the button to define the conditional call path filters. When specified, only the call path metrics matched are collected and sent to TSAM Plus manager side. This feature saves network and database resources and allows administrators to focus on exceptional cases. To specify the filter, select **Enable**. Report Previous/Next Callpath Number When it is enabled, the previous and next call paths of the matched one are also collected. You can specify the amounts of the associated call paths. The available values range is 0~100. • Metrics Evaluation Expression(s) You can select the metric, operator and threshold value to compose an expression. The logic for the expression can be "and" or "or". Following conditional filters are available: – Elapse Time exceeds a numeric value – Execution Status is or is not a value – URcode (tpreturn) is or is not a numeric value – Call depth is greater than or equal to a numeric value – Message Number on Request Queue is greater than (or equal to) a numeric value • FML Boolean Expression(s) You can also input FML Boolean expressions directly.
Dynamic Filter Panel	Dynamic filter conditions are independent of each other. If multiple conditions are configured, the evaluation is for all conditions and the monitoring can be initiated. For single condition items by default, if one of the item evaluations is, then the condition is `true`. This applies to other monitoring policy definitions unless there is a special comment.
Initiator Type List	Allows you to choose the following Initiator types: • Native Client • Workstation Client • Jolt Client • Domain Gateway • Application Server • Web Service Client • TMQFORWARD **Note** "Domain Gateway" acts as a call path initiator for local service requests. For imported services, the initiator type is set to the original caller process. The "Web Service Client" initiator point is established from the Web service gateway process (GWWS). To enable the call path monitoring for GWSNAX inbound request, you must select "Domain Gateway" when defining the policy. The WTC module is not supported for call path monitoring.
Service List	Specifies the initiator location monitored call path services. Select a service from the drop-down list. If Machine, Group, or Server is selected using an FML32 boolean expression, you must edit/ input manually.
IP Address List	Applies to workstation client and Jolt client initiator types. Specifies the IP address that initiates call path monitoring. The value can be an IPV4 or IPV6 address, or an FML32 boolean expression.
Client Name List	Lists the native client, workstation client, and Jolt client initiator type client names.
User Name List	Lists the initiator type user names.

1.2.1.1.2.4 Service Tab

The following table lists the **Service** tab options.

Table 1-8 Service Tab Options

Options	Description
Basic Policy Options	-
Enable	Enables/disables service monitoring.
Ratio/Interval	Selects Ratio or Interval policy. If multiple policies cover a single process and the ratio or interval policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. • Ratio: Accepts a value range of 1-65535. It indicates that monitoring is started among how many requests. The default value is “1” (indicating each request is monitored). • Interval: Accepts a value range of 1-65535. It indicates a period of time (in seconds) that monitoring can be started and is exclusive of ratio settings. The default value is “1”.
Alert Only	Specifies alert monitoring only. No metrics are sent to manager.
Enable Service Contract Discovery.	When this option is selected, the monitored services contract information is collected. For more information, see User Payload Collection.
Enable Payload Collection	When this option is selected, the user payload data of the monitored services is collected. For more information, see User Payload Collection.
Define Alert	Displays the alert definition page. For more information, see Tuxedo Alert Definition.
Dynamic Filter Options	-
Service List	Specifies the monitored services. Select a service from the drop-down list. If Machine, Group, or Server is selected using an FML32 boolean expression, you must edit/input manually. **Note** Oracle TSAM Plus can also monitor CORBA interfaces. For CORBA, the interface name is the same as Oracle Tuxedo ATMI services; however, "Enable Service Contract Discovery" does not apply the CORBA interface.

1.2.1.1.2.5 XA Transaction Tab

The following table lists the **XA Transaction** tab options:

Table 1-9 XA Transaction Tab Options

Options	Description
Basic Policy Options	-
Enable	Enables/disables XA Transaction monitoring.

Table 1-9 (Cont.) XA Transaction Tab Options

Options	Description
Ratio	Selects Ratio policy. If multiple policies covering a single initiator process and the ratio policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. It accepts a value range of 1-65535. It indicates that monitoring is started among how many requests. The default value is “1” (indicating each request is monitored). If transaction policy is applied to the transaction initiator process, then (similar to call path monitoring), the ratio is enforced during the initiator process. If it applies to a non-initiator transaction participator, the ratio impacts the monitored XA routines. **Note** Monitoring from the transaction initiator is recommended.
Define Alert	Displays the alert definition page. For more information, see IMS Alert Definition.
Dynamic Filter Options	-
Initiator Type List	Allows you to choose the following Initiator types: • Native Client • Workstation Client • Jolt Client • Domain Gateway • Application Server Transaction path monitoring from an initiator is currently supported. If monitoring is implemented during the initiator process, all XA Transaction points are monitored during the transaction propagation.

1.2.1.1.2.6 Domain Gateway Tab

The following table lists the **Domain Gateway** tab options:

Table 1-10 Domain Gateway Tab

Options	Description
Enable	Enables/disables Domain Gateway (GWTDOMAIN) monitoring.
Interval	Selects Interval policy. If multiple policies cover a single GWTDOMAIN process and the interval policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. It indicates a period of time (in seconds) that monitoring can be started. It accepts a value range of `1-65535`. The default value is `300`.
Define Alert	Displays the alert definition page. For more information, see Tuxedo Alert Definition.

1.2.1.1.2.7 BRIDGE Tab

The following lists the **Bridge** tab options.

Table 1-11 Sub Controls of BRIDGE Panel

Options	Description
Enable	Enables/disables Bridge monitoring.
Interval	Selects Interval policy. If multiple policies cover a single BRIDGE process and the interval policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. It indicates a period of time (in seconds) that monitoring can be started. It accepts a value range of `1-65535`. The default value is `300`.
Define Alert	Displays the alert definition page. For more information, see Tuxedo Alert Definition.

1.2.1.1.2.8 GWWS Tab

The following table lists the GWWS Panel tab options.

Table 1-12 GWWS Panel Tab Options

Options	Description
Enable	Enables/disables GWWS monitoring.
Interval	Selects Interval policy. If multiple policies cover a single GWWS process and the interval policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. It indicates a period of time (in seconds) that monitoring can be started. It accepts a value range of `1-65535`. The default value is `300`.
Define Alert	Displays the alert definition page. For more information, see Tuxedo Alert Definition.

> **Note**
>
> A policy must belong to a single domain. Oracle TSAM Plus does not support cross-domain policies. When an invalid Oracle Tuxedo domain is removed, the policies are also removed.
> All policies are global configurations that are visible for all users and editable for users with policy management administrator privileges.
>
> It is possible for a policy to be to modified *simultaneously* by multiple users. The *final changes* may not be seen by other users depending on the console refresh interval.

1.2.1.2 CICS Runtime Monitoring Policy

Oracle TSAM Plus provides comprehensive monitoring control of Oracle Tuxedo Application Runtime infrastructure behavior.

This section contains the following topics:

- Monitoring Policy List Page
- Create/Edit Policy Page

1.2.1.2.1 Monitoring Policy List Page

On the menu bar, click **Policy** and select **Tuxedo Application Runtime Monitoring Policy** from the drop-down menu. The **Monitoring Policy List** page appears. It displays existing

defined Tuxedo Application Runtime monitoring policies and allows you to view, add, edit, or delete policies.

- Button Bar
- Policy List Table

1.2.1.2.1.1 Button Bar

The following table lists the Button Bar functions.

Table 1-13 Monitoring Policy List Button Bar

Button	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns to shown in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Add	Create a new monitor policy. The maximum policy name character length is 255. You can also add a new policy by right-clicking a Domain listed in the Oracle Tuxedo Components panel.
Delete	Selected monitoring policies are deleted.
Enable	Selected monitoring policies are applied.
Disable	Selected monitoring policies are cancelled.
Edit	Edit selected monitoring policy.
Clone	Clone a new policy from a selected policy.
Import	Imports previously exported policies from a user-specified location.
Export	Exports selected policies in an file to a user-specified location.
Refresh	Updates the policies shown in the Policy List Table.

1.2.1.2.1.2 Policy List Table

The Policy List table displays the following columns:

- **Select:** Allows you to select all or individual policies.
- **Name**: Displays the current IMS policy names.
- **Status**: Displays the IMS policy status.
  - **enabled**: The corresponding request is sent to Oracle Tuxedo.
  - **disabled**: The corresponding request is not sent to Oracle Tuxedo.

> **Note**
>
> Policy monitoring does not take effect until the impacted Oracle Tuxedo processes have started.

- **CICS Region ID**: Displays the CICS region identifier (CICS region name) attached to the policy.

1.2.1.2.2 Create/Edit Policy Page

The Create/Edit Policy page contains the following sections:

- Policy Property Panel
- Tuxedo Application Runtime Monitoring Policy Panel

1.2.1.2.2.1 Policy Property Panel

The Tuxedo Application Runtime Policy panel contains the following:

- **Name**: Policy name input text box. Required.
- **CICS Region**: Selection of region that the current policy attaches to. Required.

1.2.1.2.2.2 Tuxedo Application Runtime Monitoring Policy Panel

The Tuxedo Application Runtime Monitoring Panel contains two tabs. To use the options listed in each tab, click the **Enable** check box. If enable is not selected, all options in the tab are disabled.

Following are the tabs of Oracle Tuxedo Application Runtime Monitoring Panel :

- CICS Transaction Tab
- CICS Terminals Tab

1.2.1.2.2.2.1 CICS Transaction Tab

The following table lists the **CICS Transaction** tab options.

Table 1-14 CICS Transaction Tab Options

Options	Description
Enable	Enables/disables CICS Transaction monitoring.
Ratio/Interval	Selects Ratio or Interval policy. If multiple policies cover a single process and the ratio or interval policy are different, the smaller value is used. Applies to other monitoring policy definitions as well. • Ratio: Accepts a value range of 1-65535. It indicates that monitoring is started among how many requests. The default value is 1(indicating each request is monitored). • It indicates a period of time (in seconds) that monitoring can be started and is exclusive of ratio settings. Interval: Accepts a value range of 1-65535. The default value is 1.
Alert Only	Specifies alert monitoring only. No metrics are sent to manager.
Define Alert	Displays the alert definition page. For more information, see Tuxedo Alert Definition.
Transaction List	Select monitored CICS Transaction(s) from the drop-down list or input the FML boolean expression manually.

1.2.1.2.2.2.2 CICS Terminals Tab

The following table lists the CICS Terminal tab options:

Table 1-15 CICS Terminals Tab Options

Options	Description
Enable	Enables/disables CICS Terminal monitoring.
Interval	Indicates a period of time (in seconds) that monitoring can be started. It accepts a value range of 1-65535. The default value is 300.
Define Alert	Displays the alert definition page. For more information, see CICS Alert Definition.

> **Note**
>
> A policy must belong to a single CICS region. Oracle TSAM Plus does not support cross-region policies. When an invalid CICS region is removed, the policies are also removed.
> All polices are global configurations that are visible for all users and editable for users with policy management administrator privileges.
>
> It is possible for a policy to be modified *simultaneously* by multiple users. The *final changes* may not be seen by other users depending on the console refresh interval.
>
> If the `UBBCONFIG` group setting or the `tuxgroups` in the file `Region-Group.mapping` has been modified after the ART transaction policy is defined, the resource filter might be expired. In that case, policy should be redefined.

1.2.1.3 IMS Runtime Monitoring Policy

Oracle TSAM Plus provides comprehensive monitoring control of Oracle Tuxedo Application Runtime IMS infrastructure behavior.

This section contains the following topics:

- Monitoring Policy List Page
- Create/Edit Policy Page

1.2.1.3.1 Monitoring Policy List Page

On the menu bar, click **Policy** and select **IMS Runtime Policy** from the drop-down menu. The **Monitoring Policy List** page appears. It displays existing defined Tuxedo Application Runtime monitoring IMS policies and allows you to view, add, edit, or delete policies.

- Button Bar
- Policy List Table

1.2.1.3.1.1 Button Bar

The following table lists the Monitoring Policy List button bar functions:

Table 1-16 Button Bar

Button	Description
View	From the drop-down menu, select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Add	Creates a new monitor policy. The maximum policy name character length is 255. **Note** You can also add a new policy by right-clicking a Domain listed in the Oracle Tuxedo Components panel.

Table 1-16 (Cont.) Button Bar

Button	Description
Delete	Deletes selected monitoring policies.
Enable	Enables selected monitoring policies.
Disable	Disables selected monitoring policies.
Edit	Edits selected monitoring policies.
Clone	Clones a new policy from a selected policy.
Import	Imports previously exported policies from a user-specified location.
Export	Exports selected policies in an file to a user-specified location.
Refresh	Updates the policies displayed in the Policy List table.

1.2.1.3.1.2 Policy List Table

The Policy List table displays the following columns:

- **Select:** Allows you to select all or individual policies.
- **Name**: Displays the current IMS policy names.
- **Status**: Displays the IMS policy status.
- **Domian ID**: Displays IMS policy Domain ID.

1.2.1.3.2 Create/Edit Policy Page

The Create/Edit Policy page contains the following tabs:

Click Add, Edit, or Clone, go to the Create/Edit Policy page. At the top of page, enter the name for IMS policy to be created and select a IMS Tuxedo domain.

To use the options listed in each tab, click the check box. If enable is not selected, then all the options in the tab are disabled.

- IMS Transaction Tab
- IMS Program Tab

1.2.1.3.2.1 IMS Transaction Tab

This page is used to define policy to report an IMS Transaction metric generated by MPP server.

The following table lists the **IMS Transaction** tab options.

Table 1-17 IMS Transaction Tab Options

Options	Description
Enable	Enables/disables IMS Transaction monitoring.
Ratio/Interval	Selects Ratio or Interval to collect metrics.
Alert Only	Specifies alert monitoring only. No metrics are sent to manager.
Define Alert	Displays the alert definition page. For more information, see IMS Alert Definition.

Table 1-17 (Cont.) IMS Transaction Tab Options

Options	Description
Transaction List	Select monitored IMS Transaction(s) under the Tuxedo domain from the drop-down list or input IMS transactions separated by ";" manually. If no Filter is set, this policy is available for all IMS Transactions under this IMS domain.

1.2.1.3.2.2 IMS Program Tab

This page is used to define policy to report IMS Program metric generated by BMP server. The following table lists the IMS Program tab options.

Table 1-18 IMS Program Tab Options

Options	Description
Enable	Enables/disables IMS Program metric collection.
Ratio/Interval	Selects Ratio or Interval to collect metrics.
Alert Only	Specifies alert monitoring only. No metric is sent to manager.
Define Alert	Displays the alert definition page. For more information, see IMS Alert Definition
Program List	Select monitored IMS program(s) under the Tuxedo domain from the drop-down list or input IMS programs separated by ";" manually. If no Filter is set, this policy is available for all IMS programs under this IMS domain.

1.2.2 Tuxedo Metrics Monitoring

Oracle Tuxedo Metrics collection is driven by policy monitoring. Once metrics are collected, you can view them on the related metric pages. Click **Tuxedo Metrics** on the menu bar; the **Tuxedo Metrics** page appears. From the drop-down menu you can select the following:

- Call Path
- Call Pattern
- Service
- XA Transaction
- Domain Gateway
- BRIDGE
- GWWS

1.2.2.1 Call Path

Call Path metrics monitoring provides a quick way for you to view the latest call path information. For long-running call path situations, Oracle TSAM Plus allows you to view runtime executions dynamically in real time.

The Call Path Metric window contains the following panels:

- Call Path Query by Filter Panel
- Saving and Reusing Queries
- Call Path Results Panel

1.2.2.1.1 Call Path Query by Filter Panel

The following lists the panel options. Results are displayed in the Call Path Results List panel.

Table 1-19 Call Path Query By Filter Options

Options	Descriptions
Initiator	Specifies the call path initiator type to limit the scope. You can select the following values: • Type: – All – Workstation Client – Jolt Client – Native Client – Domain Gateway – Web Service Client – Application Server – TMQFORWARD The default value is `All`. **Note** The "Initiator Type" supports multiple selections for specific initiator types. • Domain: Lists all Domains. The default value is Any. • Machine: Lists all machines for the selected domain. The default value is Any. • Server: Lists all servers for the selected machine. The default value is Any. • Initial Called Service: The first service of the call path. **Note** If the initiator type is set to "Application Server", the "Initial Called Service" value must be host service name. • Client Process Name: The initiator process name. • User Name: The Tuxedo user name is provided to call initial called service.
Message Tag	Specifies the Tuxedo Message Tag in the call path segments. **Note** To use this function, the following product versions are required: • Oracle Tuxedo 12.1.3 RP013 or later • Oracle TSAM Plus standalone 12.1.3 RP006 or later This filter only takes effect when the database type is Oracle.

Table 1-19 (Cont.) Call Path Query By Filter Options

Options	Descriptions
Status	Checks the call path status. You can select the following values: • Any • Success • Running • Application Failure • System Failure • Any Failure The default value is `Any`. **Note** "Application Failure" indicates `tperrno` is `TPESVCFAIL`. Other errors situations belong to `System Failure`.
Time	Specifies a specific time period. • Any. • Recent: Specifies the recent time period between 0~60 minutes/hours/days. Default value is 1 hour. • Time Period: Specifies a particular time span.
Min. Elapsed	Displays call paths with minimum microseconds spent (0 means all).
Max Record	Specifies the call path max number. If the query results are larger than this number, the latest max records are retrieved.

Table 1-19 (Cont.) Call Path Query By Filter Options

Options	Descriptions

Correlation ID / ECID (Optional)	This option can be used to query call path by Correlation ID or ECID. If the Execution Context ID is inputted, Oracle TSAM Plus use it to filter related call path. ECID Query works only if related Tuxedo application enables ECID.
	If the call path Correlation ID is inputted, Oracle TSAM Plus uses it to filter. The default value is empty (which indicates a Correlation ID is not used in the query).
	
	Note
	Correlation ID" query is exclusive with "Filtering Parameters":
	The Correlation ID consists of the following field values separated by a space:
	• Tuxedo domain ID: `<DOMAINID>:<master machine name>:<IPCKEY>` in the UBBCONFIG `*RESOURCE` section.
	• Logical Machine ID: `LMID` in the UBBCONFIG `*MACHINES` section.
	• Process Name:
	– "client": Used for native clients.
	– "JSH": Used for Jolt clients.
	– "WSH": Used for /WS clients.
	– <server name>: Used for the server name.
	• Process ID (pid)
	• Thread ID
	• A counter in range of 1..99999999 (starting from 1)
	• Timestamp
	
	Correlation ID Example:
	`TUXEDO:lcsol18:200401 SITE1 client 18505 1 1 1259031468`
	ECID Example:
	`004u3D6nvTI5qYSLMEo2ye0003KL000000`

1.2.2.1.2 Saving and Reusing Queries

You can save the frequently-used queries for reusing or as a base for creating similar queries. The Save/Reuse Queries area in the bottom provides the following functions:

- **Load:** Loads a saved query. When you click this button, a Saved Queries list is displayed. Select the desired query, the related conditions are loaded in the Query by Filter panel and are editable. If a historical domain, group, machine, server, or service is already removed or renamed, it is displayed in a read-only text field beneath the corresponding list or shuttle selection. It can be cleared by changing the value of the corresponding list or shuttle selection.
- **New**: Starts a new query. When you click this button, all query condition fields are reset to the default status.
- **Save**: Saves a brand new query or changes in a loaded query. Before saving a query, you must execute the query first. For a new query, when you click this button, type a unique query name and click **OK**. The saved query name is displayed as Current Query Name.
- **Save As:** Saves a loaded query to another name. Before saving a query, you must execute the query first.

- **Delete**: When a query is loaded or saved, this button is activated to delete the loaded query.

> **Note**
>
> - If a Tuxedo node (domain/machine/group/server/service) specified in a saved query that does not exist anymore (for example, removed or renamed), it can still be enquired and is displayed in the historical field in the Query by Filter panel when being enquired.
> - When a user account is deleted, all their queries saved in the system are removed.

1.2.2.1.3 Call Path Results Panel

This Call Path Results panel displays server-side call path queries. There are two sub-panels:

- Call Path Results List Panel
- Call Path Details Panel

1.2.2.1.3.1 Call Path Results List Panel

The following table lists the **Call Path Results List** panel options.

Table 1-20 Call Path Results List Panel Options

Results	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Refresh	Updates the user information list.
Detach	Displays the table in a separate window.

Table 1-20 (Cont.) Call Path Results List Panel Options

Results	Description
Call Path Data Grid	The data grid holds the entire call path information server-side query. One call path occupies one row. The columns are listed as follows: • Correlation ID. Click to display single call path details. • Root Service The first ATMI service made in the call path. • Start Time The time stamp for the start of the call path query in the following format: mmmdd,yyyy,hh:mm:ss:ms GMT • Status – Succeeded – Failed • Return Code – `TPOK/0` – `TPEXXX/tperrno` `TPEXXX` is the error code string format and `tperrno` is the corresponding numeric value, for example, `TPESVCFAIL/11`. • Elapsed Time (microsecond) The amount of time passed during the call path query. The unit is seconds with granularity to millisecond. If a call path is completed, the value is the total elapsed time used. • CPU Time (microsecond) The total CPU time used on the call path. The CPU time is the service execution CPU time summary (CPU time for multi-threaded servers cannot be accurately calculated). • User CPU Time (microsecond) The total User CPU time used on the call path. The User CPU time is the service execution User CPU time summary (User CPU time for multi-threaded servers cannot be accurately calculated). • System CPU Time (microsecond) The total System CPU time used on the call path. The System CPU time is the service execution System CPU time summary (System CPU time for multi-threaded servers cannot be accurately calculated).
–	• User return code • GTRID The XA Transaction identifier if the call path is involved in an XA Transaction. It provides the XA Transaction query results if XA Transaction monitoring is enabled. • ECID The minimum ECID if one call path has more than one ECID. • Message Tag The minimum Tuxedo Message Tag in the call path. • Client Address Client IP Address (if available). • User Name The Tuxedo user name is provided to call initial called service.
Status Bar Summary	The summary lists the following information: • Export to Excel button places the table contents into an MS Excel compatible file. • Total call path in this collection. • Running call path in this collection. • Successfully done call path number. • Application failed call path number. • System failed call path number.

1.2.2.1.3.2 Call Path Details Panel

The following table lists the **Call Path Details** panel options

Table 1-21 Call Path Details Panel Options

Results	Description
Call Path Details Data Grid	The data grid holds the entire call path server-side queries. One call path occupies one row. The columns are as follows: • Message Flow: Message Flow format: icon Server (`tpcall/tpacall/tpforward/tpconnect` Root Service) icon Server (`ARTIMS/DLI_OPERATION`) Where: • icon – Send request – Get request – Send reply – Get reply • Server: Server name **Note** – If an Oracle Tuxedo server has invoked `tpcall/tpacall/tpforward/tpconnect`, the content is displayed in parentheses. For example, `BROKER (tpcall DEPOSIT)`. – Following DLI operations are supported: `GU, GHU, GN, GHN, GNP, GHNP, ISRT, DLET, CHNG, PURG, REPL, FLD, OPEN, CLSE, INQY, POS`, and `PING`. – If OCI SQL is monitored, the `ORACLE SQL/COMMAND` is appended to Message flow, such as `simpserv1 (ORACLE SQL/SELECT)`. – If it is a `tsambegin/tsamend` node, "server process name(type/subtype)" is displayed. The type is Extended Monitoring Type specified by`tsambegin()`, and the subtype is Extended Subsidiary Monitoring Type specified by `tsambegin()`. For other columns, the detailed CICS command or SQL is displayed. • Domain: Domain call path step located. • Machine: Machine call path step located. • Group: Group call path step located. • Server: Server call path step located. • Timestamp: The logging point timestamp. • Duration (microsecond): Time span `T(n) - T(n-1)` (in seconds) • Elapsed time (microsecond): The total service elapsed time (in seconds). The default value is “hidden”. • Execution time (microsecond): The service execution time (in seconds) • Wait time (microsecond): The IPC queue wait time (in seconds). • Call Flag: The `tpcall/tpacall` call flags. • Message Size (bytes): The buffer size in bytes. • Message Queued: Number of messages in queue. • IPC queue ID: Identifies the service request queue. The default value is `hidden`. • Return Code

Table 1-21 (Cont.) Call Path Details Panel Options

Results	Description
	• User Return Code • Extended Monitoring Type: specified by `tsambegin()`. • ECID: Execution Context ID. • Tuxedo Message Tag • Others: – `LDOM` – `RDOM` – `Local GTRID` – `MSGCVTTIME`: Message Web service conversion time. – `SQL, AMOUNT, and RETURNCODE`. * `SQL`: Original SQL content after `EXEC SQL` * `AMOUNT`: This number makes sense for insert/update/delete/select only. For insert/delete/update, it indicates the number of rows affected; for select, it indicates the number of rows putted into the user buffers.`AMOUNT` is 0 when `sql open cursor` is monitored. * `RETURNCODE`: The return code retrieved from the OCI call return code by TSAM Plus agent. Unlike `SQLCODE`, `RETURNCODE` can only be got from TSAM Plus agent code. • Web service conversion time.
Status Bar	Displays the current selected call path Correlation ID. The button allows you to place the table contents into an MS Excel compatible file. Displays the current selected call path Correlation ID. The **Export to Excel** button allows you to place the table contents into an MS Excel compatible file. **Note** When exporting to Excel, if the callpath/callpattern tree is collapsed, only the nodes that are not collapsed are exported to excel file. If you want to export the full callpath/callpattern tree, you must fully expand it and then click **Export to Excel**.

Note

If multiple async calls are made in one process (for example, in a service two `tpacalls` are made), the order is based on the service invocation sequence for the reply instead of the timestamp. This allows you to easily correlate requests and reply in an "ordered" manner.
For GWWTDOMAIN, both local domain and remote domain are displayed. LDOM/RDOM information is displayed in the domain gateway cell.

For BRIDGE, the message full stages are supported (same as GWTDOMAIN).

1.2.2.2 Call Pattern

Call Pattern monitoring provides a quick way for you to view the Call Pattern information. The Call Pattern Metric window contains the following panels:

- Call Pattern Query by Filter
- Call Pattern Results Panel

1.2.2.2.1 Call Pattern Query by Filter

The following table lists the **Call Pattern Query by Filter** panel options.

Table 1-22 Call Pattern Filter Panel Options

Options	Description
Initiator	• Domain: Lists all Domains. The default value is “Any”. • Machine: Lists all machines for the selected domain. The default value is “Any”. • Group: Lists all groups for the selected machine. The default value is "Any". • Server: Lists all servers for the selected machine. The default value is “Any”. • Initial Called Service: The first service of the call path. • Client Process Name: The initiator process name. • User Name: The Tuxedo user name is provided to call initial called service.
From/To	Time Span. This option is available only when “Recent“ is not specified.
Recent	Specifies the recent time period between 0~60 minutes/hours/days. The default value is 1 hour. This option is available only when “From/To“ is not specified.
Minimum Request Number	The minimum number of requests that form a pattern. Usually a call pattern contains a large number of calls. This threshold prevents listing a pattern with a small number of calls.
Service Pattern	Checked: Displays only service call path pattern Unchecked: Displays service call path pattern including detailed location and GWTDOMAIN information

Click the **Query** button; the **Call Pattern Result List** panel appears.

> **Note**
>
> For Oracle Database, there is a lag time of minutes specified in Call Pattern Calculation Delay before you can query call patterns in one hour or day. That is, you can only query the call patterns occurred in one hour or day after the Call Pattern Calculation Delay minutes of this hour or day. For example, suppose the Call Pattern Calculation Delay is 30 minutes, if you select to query the call patterns occurred from 9 to 10 o'clock, you can actually query the desired information after 10:30, similarly, if you select to query the call patterns occurred yesterday, you can actually query the desired information after today 00:30.

- Saving and Reusing Queries

1.2.2.2.1.1 Saving and Reusing Queries

You can save the frequently-used queries for reusing or as a base for creating similar queries. For more information, refer to Saving and Reusing Queries.

1.2.2.2.2 Call Pattern Results Panel

The Call Pattern Results panel displays server-side Call Pattern queries. There are two sub-panels:

- Call Pattern Results List Panel
- Call Pattern Details Panel

1.2.2.2.2.1 Call Pattern Results List Panel

The following table lists the **Call Pattern Results List** panel options.

Table 1-23 Call Pattern Results List Panel Options

Options	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Refresh	Updates the user information list.
Detach	Displays the table in a separate window.
Call Pattern Data Grid	The data grid holds the entire call path server-side queries. One call path occupies one row. The columns are as follows: • Description: Brief information for this call pattern. Clicking it displays call pattern details as follows. • Total Number: Total number of call paths in a call pattern. • Success Number: Successful number of call paths in a call pattern. • Application Failure Number: Application failure number of call paths in a call pattern. • System Failure Number: System failure number of call paths in a call pattern. • Average Elapsed Time (microsecond): Average call pathelapsed time in a call pattern.
Status Bar Summary	Total call pattern in this collection. The **Export to Excel** button allows you to place the table contents into an MS Excel compatible file. **Note** When exporting to Excel, if the callpath/callpattern tree is collapsed, only the nodes that are not collapsed are exported to excel file. If you want to export the full callpath/callpattern tree, you must fully expand it and then click **Export to Excel**.

1.2.2.2.2.2 Call Pattern Details Panel

Click any row in the **Call Pattern** list, the selected **Call Pattern** details are displayed. The following table lists the **Call Pattern Details** panel options.

Table 1-24 Call Pattern Details Panel

Options	Description
Call Pattern Details Data Grid	The tree table data grid holds the entire call path details queried from server side. The columns are as follows: • Message Flow: Message Flow format: – ICON Service Where: – ICON – Send request Root Service: Initial service at Call Pattern For example, BR_ACNT_SUM • Domain: Domain call pattern step located. Displayed when Service Pattern is unchecked. • Machine: Machine call pattern step located. Displayed when Service Pattern is unchecked. • Group: Group call pattern step located. Displayed when Service Pattern is unchecked. • Server: Server call pattern step located. Displayed when Service Pattern is unchecked.
Status Bar	Status Bar displays the current selected call pattern index in the Call Pattern List panel. The button allows you to place the table contents into an MS Excel compatible file. The **Export to Excel** button allows you to place the table contents into an MS Excel compatible file.

1.2.2.3 Service

Service Monitoring allows you to monitor Oracle Tuxedo services. Click **Tuxedo Metrics** and select **Service** from the drop-down menu; the **Service** page appears.

The filtering options panel allows you to specify supply information to the services you want monitored. On the left, there are drop-down lists of Domain, Machine, Group and Server. There are two modes for the service selection, select the most active services or particular services on the right. The following table lists the **Service Selection** options.

Table 1-25 Service Selection Options

Options	Description
Services Selection	• Domain: Lists all Domains. The default value is “Any”. • Machine: Lists all machines for the selected domain. The default value is “Any”. • Group: Lists all server groups for the selected machine. The default value is “Any”. • Server: Lists all servers for the selected machine. The default value is “Any”. • User Name: The Tuxedo user name is provided to call initial called service.

Table 1-25 (Cont.) Service Selection Options

Options	Description
Monitoring Mode	Four monitoring modes are supported: • Most Active (Live): Allows you to query the most active services in the latest refresh-time window • Most Active (Historical): Allows you to query the most active service over a long time interval and displays the service metrics distribution during that time span. • Selected Services (Live): Allows you to monitor service dynamic execution status in the latest refresh-time window. When selected, the Available Services/Selected Services panel appears. – Available Services/Selected Services: Selects the services to be monitored. – Show services with same name as one service: If checked, specifies the query only uses the service name as the query key. If unchecked, the services are queried using the service location for same name service. – Aggregation Time: Applies to alive related queries. The algorithm is time span. – Refresh Interval: Specifies the refresh aggregation interval for service metrics computing. It only applies to live monitoring related query. • Selected Services (Historical): Allows you to query services execution status during a long time span. A time window is needed for aggregation purpose. When selected, the Available Services/Selected Services panel appears. – Available Services/Selected Services: Selects the services to be monitored. – Show services with same name as one service: If checked, specifies the query only uses the service name as the query key. If unchecked, the services are queried using the service location for same name service. – From, To: Time period. For historical query. This option is available only when “Recent“ is not specified. – Recent: Specifies the recent time period between 0~60 minutes/hours/days. The default value is 1 hour. This option is available only when “From/To“ is not specified. – Time Window: Specifies the time increment (in seconds). The default value is 3600.

Click **Query**; the query results are displayed in the **Service Monitoring Results** panel. Table1-26 lists the **Service Monitoring Results** panel options.

Table 1-26 Service Monitoring Results Panel Options

Options	Description
Metrics	From the drop-down list you can select the following service monitoring metrics: • Average Execution time (microsecond) • Success Number • Failure Number • Max Message Size (bytes) • Min message size (bytes) • Average CPU time (microsecond) • Average System CPU time (microsecond) • Average User CPU time (microsecond) • Average Message Queue Length • Average Message Wait Time in Queue (millisecond) For "CPU time", only single threaded servers are calculated (CPU time for multi-threaded servers cannot be accurately calculated). The **Pause/Resume** button allows you to stop the data refresh temporarily. The default is **Pause** (which indicates that a current refresh is in progress). Clicking it will **Resume** and refresh stops. Clicking it again restores the status.
Chart/Table	Displays results in either a chart or table. The default view is Chart (either line or bar chart). One service is one series. The horizontal axis represents the time series; the vertical axis represents the selected metrics. In table view, the **Export to Excel** button allows you to place the table contents into an MS Excel compatible file.

- Saving and Reusing Queries

1.2.2.3.1 Saving and Reusing Queries

You can save the frequently-used queries for reusing or as a base for creating similar queries. For more information, refer to Saving and Reusing Queries.

1.2.2.4 XA Transaction

There are two ways to initiate XA Transaction queries: you can specify an XA Transaction identifier, or you can query using filtering parameters. These two ways are exclusive. The following table lists the **XA Transaction Query by Scope** filtering options.

Table 1-27 XA Transaction Query by Scope Panel Options

Options	Description
Initiator Type	There XA Transaction monitoring scenarios: 1. If the monitoring policy is applied to an XA Transaction initiator, monitoring initiated with the XA Transaction path propagation (similar to Call Path). 2. If monitoring is initiated for particular processes only (such as TMS without initiator involved), propagation does not take place and only the monitored XA Transaction calls are reported. The "Initiator Type" applies to the first situation, so that a specific XA Transaction can be retrieved. It has the following values: • All • Native Client • Workstation Client • Jolt Client • Domain Gateway • Application Server The default value is `All` and the second monitoring scenario must use the default setting.
Status	Allows you to select the following values: • Any • Succeeded • Failed
Query for latest	Query under latest time (in seconds).
Query during	Query XA transactions during a specific time period.
Query by GTRID	Query an XA transaction by using an XA transaction identifier. For example `x0 x46524a28 x1`. For more information, see How the System Tracks Distributed Transaction Processing in the Oracle Tuxedo User Documentation. The **Exact Match** checkbox is under the text field. If checked, the whole identifier string must be matched, otherwise all the XA transaction IDs that contain the specified string are listed.

Click **Submit**; the XA Transaction results appears in the **XA Transaction Result List** panel.

The following table lists the **XA Transaction Results List** panel options.

Table 1-28 XA Transaction Results List Panel Options

Options	Description
GTRID	Global Transaction ID.
Initiator	The initiated process where the transaction starts.
Status	Successful transactions indicated by Failed transactions indicated by
Start Time	Time when the XA Transaction started.
Duration (microsecond)	Total transaction time span.
Execution Time (microsecond)	Total transaction time per Oracle Tuxedo service.
Parent GTRID	Displays the GTRID of the previous domain if the transaction was propagated from another Oracle Tuxedo domain.

When you click on a transaction item in the list, the transaction path, related call path ID and transaction details are displayed in the XA Transaction Path, Corresponding Call Path Correlation ID and XA Transaction Detail panels respectively.

The XA Transaction Path shows the XA Transaction network in a tree structure similar to the Component Tree. In the XA Transaction Path tree, each node represents one domain XA Transaction. If multiple /T domains are involved in the XA Transaction, the XA transaction spread path can be easily observed.

In the Corresponding Call Path Correlation ID panel, the call path(s) related to the XA transaction are listed. You can include multiple call path correlation IDs in an XA Transaction. To do so, you must define an XA Transaction policy element and a call boundary call path policy element. If the two elements are applied to one process, one XA Transaction monitoring process includes multiple call paths. Clicking on the call path ID displays the call path detail in the Call Path Metric.

The following lists the **XA Transaction Detail** panel options.

Table 1-29 XA Transaction Detail Panel Options

Options	Description
XA Routine	The transaction routine names are as follows: • `tpbegin` • `tpcommit` • `tprollback` • `tpabort` • `xa_commit` • `xa_start` • `xa_prepare` • `xa_rollback` • `xa_end` • `tms_msg_xxx (for GWTDOMAIN XA Transaction activities)` • `xa_msg_xxx (for GWTDOMAIN XA Transaction activities)`
Return Code	The XA Routine return code.
Machine/Group/Process	The XA Routine process information. The process can be an Oracle Tuxedo server or a client.
Start Time	The time when the XA Routine started.
Execution Time (microsecond)	The elapse time used for the XA Routine.

1.2.2.5 Domain Gateway

A monitoring project may contain multiple domain gateways; however, one monitoring chart can only monitor one local domain gateway (due to data source consistency). Click **Tuxedo Metrics** and select **Domain Gateway** from the drop-down menu; the **Domain Gateway Metrics** page appears. The Domain Gateway page contains two panels:

- Domain Gateway Selection
- Domain Gateway Monitoring

1.2.2.5.1 Domain Gateway Selection

The following table lists the **Domain Gateway Selection** panel options.

> **Note**
>
> Domain Gateway only supports GWTDOMAIN.

Table 1-30 Domain Gateway Selection Panel Options

Options	Description
Domain	Lists all Domains. Required.
Local Access Point	This drop-down list contains the local domain gateway configured in "Gateway" monitoring. The format is as follows: `domain id/group/server id` **Note** One group can only have one gateway instance.
Available Remote Access Point/Selected Remote Access Point	The remote domain gateway link connected with the selected local domain gateway. They are the RDOM in DMCONFIG. Multiple remote domains can be selected.
Monitoring Mode	• Live – Aggregation Time: Applies to alive related query. The algorithm is time span (in seconds). – Refresh Interval. Specifies the refresh interval for live monitoring (in seconds). • Historical – From/To: time period for historical query. – Time Window. Specifies the aggregation window for historical query (in seconds).

1.2.2.5.2 Domain Gateway Monitoring

The following table lists the **Domain Gateway Monitoring** panel options.

Table 1-31 Domain Gateway Monitoring Panel Options

Options	Description
Metrics	From the drop-down list you can select the following metrics: • Network Message Number • Network Message Bytes • Network Pending Number • Network Pending Bytes • Network Outstanding Requests
Chart/Table	Displays results in either a chart or table. The default view is Chart (either line or bar chart). One service is one series. The horizontal axis represents the time series; the vertical axis represents the selected metrics. In table view, the button allows you to place the table contents into an MS Excel compatible file.

1.2.2.6 BRIDGE

Similar to Domain Gateway.

> **Note**
>
> There is no "Network Outstanding Requests" metric.

1.2.2.7 GWWS

Click **Tuxedo Metric**s and select **GWWS** from the drop-down menu; the **GWWS Metric** page appears. The GWWS Metric page contains two panels:

- GWWS Query by Filter
- GWWS Live/History Monitoring

1.2.2.7.1 GWWS Query by Filter

The following table lists the **GWWS Query by Filter** options.

Table 1-32 GWWS Query by Filter Panel Options

Options	Description
Domain	Lists all Domains. Required.
GWWS	GWWS server list. The default is `All`.
Monitoring Mode	• Live – Aggregation Time: Applies to alive related query. The algorithm is time span (in seconds). – Refresh Interval. Specifies the refresh interval for live monitoring (in seconds). • Historical – From/To: time period for historical query. – Time Window. Specifies the aggregation window for historical query (in seconds).

1.2.2.7.2 GWWS Live/History Monitoring

The following table lists the **GWWS Live/History Monitoring** options:

Table 1-33 GWWS Live/History Monitoring Panel Options

Options	Descriptions
Metrics	From the drop-down list you can select the following metrics: • Active Thread Numbers (average active thread numbers) • Average Inbound Process Time (microsecond) • Average Outbound Process Time (microsecond) • Inbound One-Way Failure Number • Inbound One-Way Success Number • Inbound RPC Failure Number • Inbound RPC Success Number • Outbound One-Way Failure Number • Outbound One-Way Success Number • Outbound RPC Failure Number • Outbound RPC Success Number • Inbound Pending Request • Outbound Pending Request

1.2.3 CICS/IMS/Batch Runtime Metrics Monitoring

Metrics collection is driven by policy monitoring. Once metrics are collected, you can view them on the related metric pages. The Tuxedo Application Runtime Metrics page includes four panels:

To access the Tuxedo Application Runtime Metrics page, click **Tuxedo Application Runtime Metrics** on the menu bar. From the drop-down menu you can select the following:

- CICS Transactions
- CICS Terminals
- Batch Jobs
- IMS Transactions
- IMS Programs
- IMS System Traces

1.2.3.1 CICS Transactions

CICS Transactions monitoring provides a quick way for viewing the latest CICS Transaction information.

The CICS Transactions page contains the following panels:

- CICS Transactions Query by Filter Panel
- CICS Transactions Live/History Monitoring Panel

1.2.3.1.1 CICS Transactions Query by Filter Panel

The following table lists the **CICS Transactions Query by Filter** options.

Table 1-34 CICS Transactions Query By Filter Options

Options	Description
CICS Region	Lists all CICS regions. The default value is “All”.
Transaction Class	Lists all Transaction classes. The default value is “All”.
Transaction	Lists all Transactions. The default value is “All”.
Monitoring Mode	• Live – Aggregation Time: Applies to alive related query. The algorithm is time span (in seconds). – Refresh Interval. Specifies the refresh interval for live monitoring (in seconds). • Historical – From/To: time period for historical query. – Time Window. Specifies the aggregation window for historical query (in seconds).

1.2.3.1.2 CICS Transactions Live/History Monitoring Panel

The following lists the **CICS Transactions Live/History Monitoring Graph** tab metrics.

Table 1-35 CICS Transactions Live/History Monitoring Options

Options	Description
Chart Control	From the drop-down list you can select the following metrics: • Number of Transaction Calls • Average Execution Time (microsecond) • Average CPU Time (microsecond) • Average System CPU Time (microsecond) • Average user CPU Time (microsecond)
Chart/Table	Displays results in either a chart or table. The default view is Chart (either line or bar chart). One service is one series. The horizontal axis represents the time series; the vertical axis represents the selected metrics. In table view, the **Export to Excel** button allows you to place the table contents into an MS Excel compatible file.

1.2.3.2 CICS Terminals

CICS Terminals metrics provides a quick way for you to view the latest CICS Terminals information.

The CICS Terminals window contains the following panels:

- CICS Terminals Query by Filter Panel
- CICS Terminals Live/History Monitoring Panel

1.2.3.2.1 CICS Terminals Query by Filter Panel

The following table lists the options:

Table 1-36 CICS Terminals Query By Filter Options

Options	Description
CICS Region	Lists all CICS regions. The default value is "`All`".
Monitoring Mode	• Live – Minimum Policy Interval: Applies to alive related query. It is the minimum value among all Tuxedo Application Runtime monitoring policies defined (in seconds). – Refresh Interval. Specifies the refresh interval for live monitoring (in seconds). • Historical – From/To: time period for historical query. – Time Window: Specifies the aggregation window for historical query (in seconds). – Since CICS Region Start Checkbox: If checked, From/To is replaced by Start Time/Shutdown Time. – Start Time/Shutdown Time: CICS region start/shutdown time.

1.2.3.2.2 CICS Terminals Live/History Monitoring Panel

The following table lists the `CICS Terminals Live/History Monitoring` panel options.

Table 1-37 CICS Terminals Live/History Monitoring Graph Options

Options	Description
Chart Control	From the drop-down list you can select the following metrics: • Successful Transaction Number • Failed Transaction Number • Session Number
Chart/Table	Displays results in either a chart or table. The default view is Chart (either line or bar chart). One service is one series. The horizontal axis represents the time series; the vertical axis represents the selected metrics. In table view, the **Export to Excel** button allows you to place the table contents into an MS Excel compatible file.

1.2.3.3 Batch Jobs

Batch Jobs allows you to monitor the running status of the Batch Jobs. It contains two panels: Query by filter and Monitor view.

- JES Metrics Query by Filter Panel
- JES Monitor View

1.2.3.3.1 JES Metrics Query by Filter Panel

The filtering condition panel let user supply information to specify the jobs to be observed in the JES system. On the left, there are drop-down lists for JES application name, Job classes, Job priorities and Job owners, and one edit box for Job name.

There are two modes for the JES metrics monitoring, live monitoring and history monitoring.

The following table lists the UI components and their relationships.

Table 1-38 JES Metrics Query by Filter Panel

Elements	Description
JES application name	Specifies which JES system the Job is executed. The single choice dropdown list contains only live/active ones, mandatory. Same as the JES tree node name.
Job classes	Specifies one or more classes
Job name	Specifies a search a string contained in the job name.
Job priorities	Specifies one or more priorities
Job owners	Specifies one or more owners
Monitoring Mode	Two monitoring modes are supported: Live and Historical • Live Monitoring. It allows user to monitor the JES system execution status in a latest refresh window. • History Monitoring. It allows user to query JES system execution status during a long time span. A time window is needed for aggregation purpose.
Aggregation Time	Applies to history monitoring mode. The algorithm is time span
Refresh Interval	Specifies the refresh aggregation interval for JES system metrics computing. It only applies to live monitoring.

When the conditions filing is complete, click **Submit**; the monitoring results page appears on the right.

1.2.3.3.2 JES Monitor View

Table 1-39 JES Monitor View

Elements	Description
Chart Control	The "Metrics" drop down list let user select the metric aspect interested in the chart, • Successful job number in the Aggregation Time Window • Failed job number in the Aggregation Time Window • Waiting job number in different queues and the sum of all queues • Average CPU Time: – Average user CPU time for successful jobs in milliseconds int the Aggregation Time Window – Average system CPU time for successful jobs in milliseconds int the Aggregation Time Window **Note** Failed jobs do not have "Average CPU Time" Button "Pause/Resume" allows you to temporarily stop the data refresh . The default is "Pause" which means the current refresh is in progress. Clicking it again will "Resume" and the refresh stops. Clicking it again restores the status.
Chart/Table	Chart/Table will show results in style either chart or table. The chart is can be line style or bar chart. One kind of job class is one series. The horizontal axis is time series and the vertical axis is for the metrics selected.

The **Export** button allows you to save the table contents to an EXCEL compatible file.

1.2.3.4 IMS Transactions

IMS Transactions monitoring provides a quick way for viewing the latest IMS Transactions information and shows IMS transactions metrics generated by MPP server.

The IMS Transactions page contains the following panels:

- IMS Transaction Query by Filter Panel
- IMS Transaction Live/History Monitoring Panel

1.2.3.4.1 IMS Transaction Query by Filter Panel

The following table lists the **IMS Transaction Query by Filter** options.

Table 1-40 IMS Transaction Query By Filter Options

Options	Description
Domain	Lists all IMS domains. The default value is empty.
Transaction Class	Lists all Transaction classes. The default value is empty.
Transaction	Lists all Transactions. The default value is empty.
Monitoring Mode	• Live – Aggregation Time: Applies to alive related query. The algorithm is time span (in seconds). – Refresh Interval. Specifies the refresh interval for live monitoring (in seconds). • Historical – From/To: time period for historical query. – Time Window. Specifies the aggregation window for historical query (in seconds).

1.2.3.4.2 IMS Transaction Live/History Monitoring Panel

The following table lists the **IMS Transaction Live/History Monitoring Graph** tab metrics.

Table 1-41 IMS Transaction Live/History Monitoring Options

Options	Description
Chart Control	From the drop-down list you can select the following metrics: • Number of Transaction Calls • Average Execution Time (microsecond) • Average CPU Time (microsecond) • Average System CPU Time (microsecond) • Average user CPU Time (microsecond) • Average user DLI Time (microsecond)
Chart/ Table	Displays results in either a chart or table. The default view is Chart (either line or bar chart). One transaction is one series. The horizontal axis represents the time series; the vertical axis represents the selected metrics. In table view, the **Export to Excel** button allows you to place the table contents into an MS Excel compatible file.

1.2.3.5 IMS Programs

IMS Programs monitoring provides a quick way for viewing the latest IMS Programs information and shows IMS programs metrics generated by BMP server.

The IMS Programs page contains the following panels:

- IMS Program Query by Filter Panel
- IMS Program Live/History Monitoring Panel

1.2.3.5.1 IMS Program Query by Filter Panel

The following table lists the **IMS Program Query by Filter** options.

Table 1-42 IMS Program Query By Filter Options

Options	Description
Domain	Lists all IMS domains. The default value is empty.
Program	Lists all programs. The default value is empty.
Monitoring Mode	• Live – Aggregation Time: Applies to alive related query. The algorithm is time span (in seconds). – Refresh Interval. Specifies the refresh interval for live monitoring (in seconds). • Historical – From/To: time period for historical query. – Time Window. Specifies the aggregation window for historical query (in seconds).

1.2.3.5.2 IMS Program Live/History Monitoring Panel

The following table lists the **IMS Program Live/History Monitoring** tab metrics.

Table 1-43 IMS Transaction Live/History Monitoring Options

Options	Description
Chart Control	From the drop-down list you can select the following metrics: • Number of Program Calls • Average Execution Time (microsecond) • Average CPU Time (microsecond) • Average System CPU Time (microsecond) • Average user CPU Time (microsecond) • Average user DLI Time (microsecond)
Chart/Table	Displays results in either a chart or table. The default view is Chart (either line or bar chart). One program is one series. The horizontal axis represents the time series; the vertical axis represents the selected metrics. In table view, the button allows you to place the table contents into an MS Excel compatible file.

1.2.3.6 IMS System Traces

The IMS System Traces page contains the following panels:

- Search Panel
- Query Result List Table
- Detailed Information Panel

1.2.3.6.1 Search Panel

The following table lists the query filters on the Search panel.

Table 1-44 Query Filters

Options	Description
Domain	Lists all IMS domains. The default value is empty.
Machine	Lists all the machines belong to the selected domains. The default value is empty.
Group	Lists all the groups belong to the selected machines. The default value is empty.
Server	Lists all the servers belong to the selected groups. The default value is empty.
Transaction Class	1 ~ 999. The default value is empty.
Transaction	Lists all the transactions belong to the selected domains. The default value is empty.
Program Name	Lists all the programs belong to the selected domains. The default value is empty.
Region Type	MPP and BMP. The default value is empty.
From / To	The transaction/program ending time span. The default value is latest 24 hours.
Max Queried Out Record	Limits the returned record number. Default is 500. Too large value in this field may cause browser out of response

Clicking on the **Reset** button resets all the query filters (except Max Queried Out Record) to the initial status.

1.2.3.6.2 Query Result List Table

When clicking the **Query** button, all the Transaction/Program collect instances met the search criteria are listed in the Query Result List table. Click any of the entries listed in the Query Result List table to display the detailed information in the Detailed Information panel.

Clicking on the **Refresh** button executes the last query once more and loads the latest DB data in the list table.

1.2.3.6.3 Detailed Information Panel

This panel displays the detailed information of the entry selected in the Query Result List Table. The following table lists the detailed information:

Table 1-45 Detailed Information

Name	Description
Domain	Tuxedo domain ID
Machine	Machine name
Group	Group name
Server	Server name
Server ID	Tuxedo server ID
PID	Server PID
Transaction Class	IMS transaction class
Transaction Name	IMS transaction name
Program Name	IMS program name
Logic Terminal	Logic terminal name
Region Type	The IMS region type, MPP or BMP
UserID	OS user ID
Start Time	IMS transaction/program start time point

Table 1-45 (Cont.) Detailed Information

Name	Description
End Time	IMS transaction/program stop time point
Elapsed Time	IMS transaction/program elapsed time from start to end (microseconds)
System CPU Time	System CPU time (microseconds)
User CPU Time	User CPU time (microseconds)
PSB Name	IMS PSB name
Program Elapsed Time	IMS program elapsed time (microseconds)
Current SPA Size	SPA size
Abend Code	Program abend code
Elapsed Time in DL/I	Total time elapsed in DL/I (microseconds)
Enqueue Number	Message number pushed in /Q
Dequeue Number	Message number popped from /Q
DLI Summary Information	The DLI summary information is presented by a table. One transaction/program may contain one or multiple DLI entries. There are four columns of the table, DL/I Event Name, DL/I Type, DL/I Invoked Count, and DL/I Total Duration (microsecond).

1.2.4 CICS/IMS/Batch Management

- Batch Jobs Submit
- Batch Jobs Search/Display
- Batch Syslog Search/Display
- CICS Resources View/Edit
- IMS Resources View/Edit

1.2.4.1 Batch Jobs Submit

JES Job submit provides a quick way for you to submit a job through the TSAM Plus console. For more information, see Oracle ART Runtime documentation Oracle ART Runtime documentation.

> **Note**
>
> To enable JES job submit and monitoring, you must set the `JESMONITOR` environment variable to yes before you start the LMS server and set the "`JOBREPOSITORY`" value in the JES configuration file to specify the path of the job repository.
> If the "`JOBREPOSITORY`" value is not in the JES configuration file, the list panel lists the JOB in the `APPDIR`.

The JES job submit window contains the following panels:

- JES Application Selection Panel
- Job File Information List Panel

1.2.4.1.1 JES Application Selection Panel

Click **List Available Jobs**, all available job script files are listed in the Job File Information List Panel" if the selected JES application is alive.

1.2.4.1.2 Job File Information List Panel

The following table lists the JES Job File Information List Panel options.

Table 1-46 Job File Information List Panel Options

Options	Description
Script Name	Job script file name.
Name	Job name.
Priority	Job priority.
Class	Job class. Value may be [A-Z], [0-9]
Restart Option	The name of the step to use to restart the job
Type run	Indicates what should be done with the job. Choose one of the following: • COPY - Copy the job directly in an output stream to sysout. • HOLD - The system should hold the job. • JCLHOLD - JES should hold the job. • SCAN - Scan JCL for syntax errors only.
Version	The EJR runtime engine version.
Start label	The label of the first phase to be started
EJR Option	Enter the EJR Option you want to start the job with.
Shell Option	Enter the Shell Option you want to start the job with.

Select an item, and click **Submit**. If the job is submitted successfully, the display message appears as follows:

"Submit of Job xxxx was successful", where "xxxx" is the job id. Click **View Job** to see a detailed message. If it fails, an error message is displayed.

1.2.4.2 Batch Jobs Search/Display

JES Jobs metrics provides a quick way for you to view the latest JES jobs information.

The JES jobs window contains the following panels:

- JES Jobs Query by Filter Panel
- Jobs Query Results List Panel
- Job Detail Information Panel

1.2.4.2.1 JES Jobs Query by Filter Panel

The following table lists the **JES Jobs Query by Filter** options.

Table 1-47 JES Jobs Query By Filter Options

Elements	Description
JES application	Specifies which JES system the Job is executed,. The single choice dropdown list contains only live/active ones, mandatory. Same as the JES tree node name.
Job classes	Specifies one or more classes
Job name	Specifies a search a string contained in the job name.
Job priority	Specifies one or more priorities
Job owners	Specifies one or more owners separated by a semi-colon (or a coma (,).
Job status	Specifies one or more of the following status categories: • EXECUTING • CONVING • WAITING • DONE • FAIL • HOLD_WAITING • HOLD_CONVING • INDOUBT • DISCARD
Submitted in latest _ seconds	Query the most recent Jobs submitted in latest a few seconds
Submit during	Query JES Jobs submitted during a specific time period.

You can also query the exact job ID by using 'Query by Job ID' subform. Fill in 'Job ID' and click **Query**; if found, the corresponding job is listed in the result.

1.2.4.2.2 Jobs Query Results List Panel

The following table lists the **JES Jobs Query Results List** table columns.

Table 1-48 Jobs Query Results List

Sort Options	Description
Name	Job name.
ID	Job ID
Node	Machine name
Owner	The person that submitted the job
Priority	Job priority.
Current Queue	The current queue where the job is placed.
Class	Job class. Value may be [A-Z], [0-9]
Submit Time	Time when the job was submitted.
End Time	Time when job completes.
Status	Job status.

Certain actions can be made to the queried out job list entries. Besides the **Refresh** button, **Cancel**, **Purge**, **Hold**, and **Release** actions can be used on selected jobs. The job cancel and purge behavior is the same same as the `artjesadmin` command. The command return status is displayed in a popup window.

> **Note**
>
> A job can be held only when the status is `CONVING` or `WAITING`.
> A job can be released only when the job status is `HOLD_WAITING`.
>
> A job can be purged only when the job is not in the `PURGE` queue.

Two additional actions/buttons (**Job Logs** and **Job Sysouts**) are located on the button bar that provide job log and job sysout information.

> **Note**
>
> If job logs or job sysouts exceed 10, 000 bytes, the file is truncated (that is, only the last 10,000 bytes are retained).
> Purged jobs do not have Job Logs and Sysouts to view

All records in the job list table can be exported to a `.xls` file by clicking the **Export to Excel** button below the list table.

> **Note**
>
> If you are using Internet Explorer, and IE security is set above medium, a warning message pops up when you click the **Export to Excel** button. Click the export button again to ignore the warning.

- Choosing Monitoring Mode

1.2.4.2.2.1 Choosing Monitoring Mode

You can change monitoring to auto refresh mode by specifying the Refresh Interval in the query result list panel toolbar; auto refresh is disabled by default. The refresh rate can be set as follows:

- 1 minute
- 5 minutes
- 10 minutes
- 30 minutes
- 60 minutes
- 120 minutes

1.2.4.2.3 Job Detail Information Panel

When you select a Job in the Job Query Results List table, detailed information for the selected job is displayed in the Job Detail Information panel. The job detailed information is self-explanatory and includes the following:

- Running step
- Running time

- Current queue
- Status
- Type Run
- Initiator
- End Time
- User CPU usage
- System CPU usage

> **Note**
>
> Job detail information is retrieved along with the Job Query List; the content may not reflect the latest information. To view the latest job details, click the refresh button.

1.2.4.3 Batch Syslog Search/Display

Oracle TSAM Plus allows you to query the Batch JES system log.

The Batch Syslog window contains the following panels:

- JES Syslogs Query by Filter Panel
- JES Syslogs Query Results Panel

1.2.4.3.1 JES Syslogs Query by Filter Panel

The following table lists the JES Syslogs Query by Filter options.

Table 1-49 JES Syslogs Query by Filter Options

Options	Description
JES Application	Specifies the JES system by which the JES syslog is shows
Job Name	Specifies a search string contained in the job name
Generated in Latest	Query syslog generated in the latest few seconds
Generated During	Query syslog generated during a specific time period

You can also query the exact syslog using the related job ID. In the field **Query by Job ID**, fill in the job ID and click **Query**. The corresponding syslog is listed in the results if searched.

1.2.4.3.2 JES Syslogs Query Results Panel

By default, only the latest 5000 lines of Batch JES syslog are shown. If there are more logs in your system, you can click the Prev chunk or Next chunk button to view the previous or next 5000 lines (the size of chunk) of the system logs.

In the current chunk, you can click the First/Prev/Next/Last page button to browse the system logs.

1.2.4.4 CICS Resources View/Edit

Oracle TSAM Plus allows you to query and edit CICS resource configuration files on the Oracle Tuxedo master node.

> **Note**
>
> To enable this function, you must make sure the ARTADM server runs on each node and the `KIXCONFIG` environment variable is set to the CICS resource files directory.

- Querying CICS Resources
- Editing/Viewing CICS Resources

1.2.4.4.1 Querying CICS Resources

You can query CICS resources by region. All of the CICS Resource configuration files are listed after you select a CICS region and click the **Query** button. You can also click **Refresh** button to refresh the CICS Resource list for the selected CICS region.

1.2.4.4.2 Editing/Viewing CICS Resources

You can edit or view the CICS resource depending on the authority configured in User Management.

To edit the CICS Resource configuration file, you must do the following steps:

1. Select one CICS region from region dropbox, then click the **Query** button. All of the CICS configuration files belonging to the selected region are listed.
2. Select a configuration file then click the **Edit** button.

> **Note**
>
> The **Edit** button is enabled when the number of selected configuration file is 1.

3. Click the **Update** button to save the modification. You can also click the **Back** button to return to the list of CICS Resources without modifying the file.

> **Note**
>
> If there are any format errors in the listed files, an error message is displayed.

For more information, see Oracle Tuxedo Application Runtime for CICS and Batch documentation.

1.2.4.5 IMS Resources View/Edit

Oracle TSAM Plus allows you to query and edit IMS resource configuration files on the Oracle Tuxedo master node.

- Querying IMS Resources

- Editing/Viewing IMS Resources

1.2.4.5.1 Querying IMS Resources

You can query IMS resources by IMS domain. All of the IMS Resource configuration files are listed after you select an IMS domain and click the **Query** button. You can also click **Refresh** to refresh the IMS Resource list for the selected Tuxedo domain.

1.2.4.5.2 Editing/Viewing IMS Resources

You can edit or view the IMS resource depending on the authority configured in User Management.

To edit the IMS Resource configuration file, you must do the following steps:

1. Select one IMS domain from IMS Domain drop down list, and then click the **Query** button. All of the IMS configuration files belonging to the selected domain are listed.
2. Select a configuration file then click the **Edit** button.

> **Note**
>
> The **Edit** button is enabled when the number of selected configuration file is 1.

3. Click the **Update** button to save the modification. You can also click the **Back** button to return to the list of IMS Resources without modifying the file.

> **Note**
>
> If there are any format errors in the listed files, an error message is displayed.

For more information, see Oracle Tuxedo Application Runtime for IMS documentation.

1.2.5 User/Data Management

Click **Management** and select the following from the drop-down list:

- User Management
- Data Management
- Global Parameters
- Blackout
- Domain Group Management

1.2.5.1 User Management

The User List page allows you to add, edit and delete users and groups. An Oracle TSAM Plus group is a set of privileges. The default groups are "administrator" and "viewer". They cannot be deleted.

An Oracle TSAM Plus user may belong to one or more groups. When Oracle TSAM Plus is installed, the default user is “admin” (configured during installation), and cannot be deleted.

You can enter the **Group List** menu bar by clicking the **Group List** button, and return to the **User List** menu bar by clicking the **User List** button.

The following table lists the **User List Menu Bar** options.

Table 1-50 User List Menu Bar Options

Elements	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Change Properties	Allows you to change user properties (if proper permission is set) after login to the system. You can change all user properties from the User Management window if you have User Management administrator privileges. Select the user you want to edit and click the **Change Properties** button. If you are the selected user, you can change your own properties. The current property settings are shown in the corresponding text fields. Type new values for the following properties: • Full Name • Description • Group
Change Password	Allows you to change user password (if proper permission is set) after login to the system. Enter your old password, then enter the your new password. The password should be limited to 6~16 characters, and can contain the following characters: alphanumeric characters, underscores. You can change all user passwords from the User Management window if you have User Management administrator privileges. Select the user whose password you want to change and click the **Change Password** button. If you are the selected user, you can change your own password. Click **Change Password** to change the password. Click to cancel the operation and return to the User Management window. **Note** The TSAM Plus user password is valid for 180 days. You need to change your user password before it is expired. If the password has expired, you can find related information recorded in the `tsam.log` file.

Table 1-50 (Cont.) User List Menu Bar Options

Elements	Description
Create User	Allows you to add a new user. You must enter the following: **Note** The **Create User** button is enabled only when the current logged-in user has User Management administrator privileges. • Name(*) The user login name. User name should be limited to 5~16 characters, and can contain the following characters: "[a-z], [A-Z], [0-9], _". The initial character must be [a-z] or [A-Z]. • Full Name The user full name. User full name should be limited to 128 characters, and can contain the following characters: alphanumeric characters, underscore, space, or period. • Password(*) User password. You need to provide password and confirm password. The password should be limited to 6~16 characters, and can contain the following characters: alphanumeric characters, underscores. • Description The users description. The description is limited to 255 characters, and can contain the following characters: alphanumeric characters, underscore, space, or period. • Group(*) A drop-down list. A created user can belong to on or more groups.
Delete User	Deletes the selected user.
Online User	The information of all online users is displayed in window. The available information of users includes Name, IP Address, Login Time and Session ID.
Refresh	Updates the user information list.
Detach	Displays the table in a separate window.

The following table lists the **Group List** button bar options.

Table 1-51 Group List Button Bar Options

Elements	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Modify	Allows you to change group properties The **Modify** button is enabled when the current login user has the administrator privilege of group management. Select the group you want to edit and click the **Modify** button. The current property settings are shown in the corresponding text fields of the window. Type new values for the following properties: • Description • Privileges

Table 1-51 (Cont.) Group List Button Bar Options

Elements	Description
Create Group	Allows you to add a new group. You must enter the following: **Note** The Create Group button is enabled when the current logged-in user has User Management administrator privileges. The privileges you need to set are displayed below the input bar and listed in • Name(*) The group name. Group name should be limited to 5~16 characters, and can contain the following characters: "[a-z], [A-Z], [0-9], _". The initial character must be [a-z] or [A-Z]. • Id The group Id. It should be an integer and not less than 0. • Description The group description. The description is limited to 255 characters. It can contain the following characters: alphanumeric characters, underscore, space, or period. • Privileges(*) A table. Allows you to set group privileges.
Delete Group	Deletes the selected group. A group cannot be deleted if there are any users who belongs to it.
Refresh	Updates the group information list.
Detach	Displays the table in a separate window.

Note

When OpenID Connect (OIDC) authentication is enabled, the application disables its local user management interface. The 'User Management' menu is replaced with 'Online Users', as user provisioning and lifecycle management are delegated to the configured Keycloak server.

1.2.5.2 Data Management

Data Management allows you to purge the Oracle TSAM Plus database data (including the monitoring data in the database and the invalid Oracle Tuxedo components in the database).

- Purging Monitoring Metrics Data
- Purging Invalid Tuxedo Components Nodes

1.2.5.2.1 Purging Monitoring Metrics Data

You can purge all monitoring data including Server/Service data and Call Path/ XA Transaction data. To purge Monitoring data, do the following steps:

1. Select the Types you want purged.
   - All
   - Call Path
   - Bridge

- GWTDOMAIN
- Service
- XA Transaction
- User payload metrics
- GWWS
- Alert
- Tuxedo CICS Terminals
- JES
- IMS

> **Note**
>
> - If you want to purge Tuxedo CICS Transaction data, "Service" type can be selected.
> - Only user payload metrics stored in TSAM plus database can be purged here. User payload metrics stored in Hadoop or local file can only be purged by the user manually.
> - Purging call path or service metrics does not delete the corresponding user payload metrics.

2. Set the **Old Than** date, before which the monitoring data will be purged.
3. Click the **Purge** button to delete monitoring data from the database.
   The statistics service metrics data are purged automatically:
   - Raw data are purged after 7 days.
   - Hourly aggregated data are purged after 32 days.
   - Daily aggregated data are purged after 12 months.

1.2.5.2.2 Purging Invalid Tuxedo Components Nodes

Tuxedo components can be changed to "`INValid`" status due to management operations at Tuxedo application side. By default, the "`INValid`" Tuxedo components are not deleted from the database. Customers can purge all "`INValid`" Tuxedo components in the Data management window.

> **Note**
>
> Currently, only the purging all "INValid" Tuxedo components on the data management page is supported. Invalid components can be purged in the component tree.

1.2.5.3 Global Parameters

The Global Parameters page contains following tabs:

- TSAM Plus Global Properties
- TSAM Plus Manager Properties

1.2.5.3.1 TSAM Plus Global Properties

The following table lists the TSAM Plus Global properties.

Table 1-52 TSAM Plus Global Properties

Properties	Description
TSAM Plus User password Life Time(days)	The period of time, in days, that a user password is in effect. Its value can be 0~2147483647. The default value is 180 days. If specified to 0, the password will never expire.
Maximum Selected Services in Service Metrics	The maximum selected services in Service Metrics.
Call pattern calculation schedule	The period of statistics job run for Call Pattern. The valid value is DAILY or HOURLY. DAILY is the default value. The modifications of this parameter take effect immediately. This parameter is applicable for Oracle Database only. If TSAM Plus database is Derby, it is invisible.
Call pattern calculation delay (minutes)	The delay minutes after one hour or day for statistics job run for Call Pattern. If schedule is HOURLY, the valid value is 10~59, and 30 is the default value. If schedule is DAILY, the valid value is 10~1439, and 120 is the default value. The modifications of this parameter take effect immediately. This Parameter is applicable for Oracle Database only. If TSAM Plus database is Derby, it is invisible.
Automatic data purge	Automatically purge data or not. FALSE is the default value. The modifications of this parameter is stored in Oracle database immediately. If **Automatic data purge** is TRUE, the expired monitoring data is purged at time by the value of **Daily Maintenance Every Day**. This Parameter is applicable for Oracle Database only. If TSAM Plus database is Derby, it is invisible.
Reserve monitoring data for days	Days for data to be reserved before purging. If purge is FALSE, it is set to `-1` and is not editable. If purge is TRUE, its valid value is 0~2880. The modifications of this parameter is stored in Oracle database immediately. If **Automatic data purge** is TRUE, the expired monitoring data is purged at time by the value of **Daily Maintenance Every Day**. This Parameter is applicable for Oracle Database only. If TSAM Plus database is Derby, it is invisible.
Daily Maintenance Every Day	Change the schedule when Oracle Database daily maintenance job (`TSAM_JOB_DAILY`) executes. `TSAM_JOB_DAILY` purges expired monitoring data if **Automatic data purge** is TRUE.
Statistics Collection Interval (minutes)	Specify the interval to collect the statistics metrics data presented in dashboards. For more information, refer to Domains Dashboard.
Payload Storage	Select one of the user payload data storage: Database, Hadoop, or local file.
Hadoop URL	Specify the Hadoop URL where you want to storage the user payload data. The Hadoop URL must include the hostname, port, and payload file directory. For example: `hdfs://localhost:8080/tmp/tuxPayload/` If the URL is invalid or unreachable, a warning message is displayed.

1.2.5.3.2 TSAM Plus Manager Properties

The following table lists the TSAM Plus Manager properties for each panel.

Table 1-53 Manager Parameter Properties

Properties	Description
Default Top N of Services	The number of most active services on Service Monitoring page. The default value is 2.
Tuxedo Application Runtime Feature Enabled Check Box	Indicates if Oracle Tuxedo Application Runtime related components/ pages are displayed on TSAM Plus console. **Note** If you check or unchecked **Tuxedo Application Runtime Feature Enabled**, you must restart the Oracle TSAM Plus application for the change to take effect.
Synchronous Query Timeout (seconds)	Allows you to set the JES Job query timeout value (in seconds). The default value is 30 seconds.
Configuration Files Backup Directory	The directory for configuration files backup. The default path is `$USER_INSTALL_DIR$`. **Note** To back up configuration files successfully, properly set the file permission of the backup directory, or start up TSAM Plus Manager web server using the same account as the backup directory file owner
Max Persistence Threads	Denotes how many persistence threads in a persistence thread pool. This number should not be bigger than the CPU number of the host running the Data server of TSAM Plus manager. The default value is 2.
Data Persistence Queue Size	The maximum of the metric entity list in the persistence queue before traffic control. The default value is 5000.
Queue Full Sleep Interval (milliseconds)	The default value is 500.
Max JVM Memory Threshold (%)	When the memory usage of the JVM which runs TSAM Plus Manager exceeds this threshold, TSAM Plus Manager rejects metrics data reported by LMS.
Property: Max JVM Memory Threshold (%)	When the memory usage of the JVM which runs TSAM Plus Manager exceeds this threshold, TSAM Plus Manager rejects metrics data reported by LMS.
Queue Full Sleep Interval (milliseconds)	Denotes the LMS sleep interval (in milliseconds) in case the value of Data Persistence Queue Size is exceeded. The default value is 500. If the value of Data Persistence Queue Size is exceeded, TSAM Plus Manager persistence threads process the data metric as normal, and at same sends LMS a response with sleep interval (in milliseconds). LMS sleeps for the interval before sending another data metric.

Table 1-53 (Cont.) Manager Parameter Properties

Properties	Description
Timeout Shutdown (seconds)	Denotes the timeout (in seconds) to give metric entity persistence threads a chance to finish their job after you shutdown the Oracle TSAM Plus manager. The default value is 30.
Enable DYNAMIC_RAP	Denote if `DYNAMIC_RAP`(configure in `BDMCONFIG`) feature Oracle Tuxedo JCA Adapter should be supported or not. If this parameter is enabled, the remote JCA adapter domain connected by `DYNAMIC_RAP` can be selected from domain gateway monitored page.
TSAM Plus Manager Log Level	Log level control for TSAM Plus Manager. The default value is Info. (Trace, Debug, Info, Warn, Error). Log level modifications take effect immediately; you do not need to reboot the application server.
JPA SQL Log Level	Log level control for JPA SQL. The default value is Warn. (Trace, Debug, Info, Warn, Error). Log level modifications take effect immediately; you do not need to reboot the application server.

Clicking on the **Modify Command** button saves the modifications into DB or properties file. If you need to reboot the TSAM Plus Manager, you can get the information in pop-up box.

Clicking on the **Refresh** command loads current value of each property from DB or properties file.

1.2.5.4 Blackout

With the Blackout management feature, users can easily control the metric data collection schedule. Once a Blackout starts, there is no metric data communication between TSAM Plus manager and agent. Blackouts can be started or ended immediately, or according to a specific schedule.

- List Blackout Definitions
- Add/Edit a Blackout Definition

1.2.5.4.1 List Blackout Definitions

Blackout List panel lists all the defined blackout definitions. Blackout policy is enabled on domain level. The blackout list contains the following information for each blackout definition:

Table 1-54 Blackout List Table Content

Column	Description
Select	The selection checkbox.
Blackout Name	Globally unique Blackout name.
Domain ID	On which domain the Blackout defines.
Status	Enabled/Disabled. This status indicates whether this blackout is enabled.

Table 1-54 (Cont.) Blackout List Table Content

Column	Description
Schedule Summary	Show the Blackout schedule summary. Policy content is organized in xml, each policy have following child nodes. • starttime: start time in seconds. • duration: duration time in seconds.-1 for infinite • endtime: end time in seconds.-1 for no end time • repeattype: repeat type. • repeatvalue: repeat value. Default value is 0. • heartbeat: heart beat interval.-1 for stopping heartbeat

> **Note**
>
> Blackout Name and Policy Name must be different as they share the same naming space.

The following table lists the actions you can take:

Table 1-55 Blackout List Table Controls

Control	Description
Add	Adds Blackout schedule on specific domain(s). The Blackout creation is done in the Edit Blackout page.
Delete	Removes defined Blackout on the selected domain(s). Blackout on this domain is removed if the connection between agent and manager is OK.
Enable	Enables the selected Blackout(s) immediately.
Disable	Disables the selected Blackout(s) immediately.
Edit	Edits the Blackout definition. The control is disabled when multiple Blackouts are selected.
Clone	Adds a new Blackout with the same schedule of the selected one. The control is disabled when multiple Blackouts are selected.
Refresh	Refreshes the table.

1.2.5.4.2 Add/Edit a Blackout Definition

On clicking of the **Create** or **Edit** button in the **Blackout List** table, the **Create/Edit Blackout** page is shown. The following table lists the fields that should be filled to define a Blackout schedule.

Table 1-56 Create/Edit Blackout Fields

Field	Options	Description	Validation
Name	-	Globally unique Blackout name.	It cannot exceed 255 characters.
Domain	-	The corresponding Domain.	-
Heartbeat Frequency	-	Agent send heart beat frequency. Agent do not send heart beat if this check box is not chosen.	-
Start	Immediately	Blackout start time. It's converted to TSAM Plus manager current time when user save this blackout.	-

Table 1-56 (Cont.) Create/Edit Blackout Fields

Field	Options	Description	Validation
	Later	Specify the Blackout start date/time.	A valid date string
Duration	Infinite	No end Blackout.	-
	Length	How many hours and minutes the Blackout last.	Hour should be a number and in range (0,1000000). Minutes should be a number and in range (0,59) Hours and Minutest should not be zero at the same time.
	Until	Until the designated time.	A valid date string
Repeating	Type	At what frequency the Blackout repeats. "By minutes","By Hours","By Days". "Weekly","Monthly".	-
	Frequency	Repeat period.	It should be a number and in range (0,1000000)
End Date	No End Date	Infinite repeating.	-
	Specified End Date	Specify the repeating end date/time.	A valid date string

> **Note**
>
> TSAM Plus Manager should be synchronized with agent. All time inputted in TSAM Plus console is taken as the time zone of TSAM Plus Manager.

Add and **Add & Enable** buttons are shown when you create a new blackout.

Save and **Save & Enable** buttons are shown when you edit an existing blackout.

- Add
  Save the Blackout schedule configuration, start the Blackout immediately if "Immediately" is configured, or schedule it for later run.
- Add & Enable
  Save and enable blackout, then back to the Blackout List Page.
- Save
  Save the modified Blackout schedule configuration, start the Blackout immediately if "Immediately" is configured, or schedule it for later run.
- Save & Enable
  Save and enable the modified Blackout schedule configuration.
- Cancel
  Cancel the Blackout creation/edition and back to the **Blackout List** page.

1.2.5.5 Domain Group Management

The Domain Group Management page allows you to create and manage domain groups. A domain group can be monitored in the domains dashboad.

- Viewing Domain Group List

- Creating a New Domain Group
- Editing a Domain Group

1.2.5.5.1 Viewing Domain Group List

The Domain Group List shows all the domain groups created. The following table lists the information you can view for each group.

Table 1-57 Domain Group List

Items	Description
Name	Domain group name
Domain Count	The number of domains included in the group
Domains	The name of domains belonging to the group
Key Services	Key services defined in the group. The key services is a set of services you want to monitor regularly from the domains dashboard.

1.2.5.5.2 Creating a New Domain Group

To create a new domain group, do the following:

- From the Domain Group List, click **Add.**
- In the window that appears, specify the following and click **OK**.
  - Domain Group Name: Define a group name
  - Domain Selection: Select the domains you want to include in the group
  - Key Services: Optional. Select up to seven services that you want to monitor regularly from the group dashboard. Only the services that are available across all domains can be selected.

1.2.5.5.3 Editing a Domain Group

To edit a domain group, do the following:

- From the Domain Group List, highlight the group you want to edit.
- Click **Edit.**
- Specify the domains and key services, and then click **OK**.

1.2.6 Load Generator

You can create the replay definition from call paths by Clicking **Load Generator ->Replay Definition**. Based on the replay definition, you can execute the replay for standard and stress test modes. For more information, see Using Test Load Generator.

1.2.7 Alert Monitoring

Click **Alert** and select one of the following:

- Tuxedo Alert Definition
- CICS Alert Definition
- IMS Alert Definition

- Batch Alert Definition
- Alert Query
- System Alerts Supported
- Alert Metrics Tables

1.2.7.1 Tuxedo Alert Definition

Click **Alert** and select **Tuxedo Alert Definition** from the drop-down list; the Tuxedo Alert Definition List Panel appears. This panel lists available alert definitions and allows you to create, edit, and manage alert definitions.

The following tables list the **Tuxedo Alert Definition Menu Bar** and **Tuxedo Alert Column** options respectively.

Table 1-58 Tuxedo Alert Definition Menu Bar Options

Options	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns displayed in the table. • Detach: Displays the table in a separate window. • Reorder Columns: Change how the column order is displayed.
Add	Creates a new alert definition.
Delete	Deletes the alert definition.
Enable	Enables the alert definition.
Disable	Disables the alert definition.
Edit	Modifies the alert definition.
Clone	Creates a new alert with same definition as current alert but the name is left empty.
Alerts	See all alerts generated by this alert definition.
Refresh	Refresh the alert definition list.
Detach	Displays the table in a separate window.

Table 1-59 Tuxedo Alert Columns

Column	Description
Selection checkbooks	Select a set of alert definitions in current page for processing.
Name	The alert name specified in the alert definition.
Status	Displays alert status. The status could be enabled or disabled. Enable: The alert definition enabling request has been sent to Oracle Tuxedo. Disable: The alert definition disabling request has been sent to Oracle Tuxedo.
Type	The monitoring category and system are consistent with policy definition. The category types are as follows: • Call Path • Service • XA Transaction • BRIDGE • GWTDOMAIN • GWWS • Service Statistics: a `default_adaptive_alert` is enabled by default.
Evaluation Condition	The FML Boolean expression of the alert triggering conditions
Tuxedo Components	The resource FML Boolean expression (similar to Policy definition).

- Define New Alert Page
- Adaptive Settings (For Service Statistics Alerts Only)

1.2.7.1.1 Define New Alert Page

Click the **Add**, **Edit** or **Clone** button on the **Alert Definition List** Menu bar; the **Define New Alert** page appears. It allows you to define a concrete Oracle Tuxedo alert definition.

The Define New Alert page is divided into the following four sections:

- Alert Properties
- Tuxedo Components
- Metrics Evaluation Expression(s)
- FML Boolean Expression(s)

1.2.7.1.1.1 Alert Properties

The following table lists the **Alert Properties** options.

Table 1-60 Alert Properties Options

Options	Descriptions
Name	The name of the alert. It must be unique among the alerts globally. The name value is limited to 255 characters and must be unique within the project. The initial character must not be "."
Type	The type of the alert; it is based on monitoring policy. The drop-down list includes the following items: • Call Path • Service When you select a service alert, the Metrics Independent Checking check box appears. It allows Oracle TSAM Plus to check service timeouts independent of metrics collection. The alert can be generated while the service is running. If checked, “Drop Message” is removed from the “Action” option drop-down menu. • Service Statistics You can define one or more service statistics alerts for a Tuxedo domain or a domain group. When you select a service statistics alert, the configuration panel becomes different than other alert types. You can configure TSAM Plus to compare the instant metric data with a static threshold or historical data to evaluate and trigger the service statistics alerts. For more information, see Adaptive Settings (For Service Statistics Alerts Only). • XA Transaction • GWTDOMAIN • BRIDGE • GWWS
Severity	The severity drop-down list contains the following severity levels: • Fatal • Critical • Warn • Information
Interval	Accepts an integer value in seconds. The current alert is evaluated only once during this interval. The purpose is to throttle alert volume in similar scenario. If the interval value is 0, any alert is reported.

Table 1-60 (Cont.) Alert Properties Options

Options	Descriptions
Action	Specifies what kind of action is executed when an alert definition is set to "true". The following actions are supported: • Publish to Tuxedo Event Broker An event is posted to the Oracle Tuxedo event broker. The event name is the alert name by default; you can also specify it manually. The buffer is an FML32 buffer containing the metric snapshot. • Drop Message If this alert evaluation is true, the request message is dropped and the call fails (TPESYSTEM). This only applies to Call Path and Service type alerts. The evaluation points come before the request sent to the IPC queue (call path) and after it is retrieved from the IPC queue (call path, service). This alert can be used to avoid unneeded service processing for stagnant requests. For example, if the request message "Wait Time" in the IPC queue exceeds a particular threshold, the client may have already timed out. In this case, the action can drop the stagnant request and the application server will not process it. **Caution**: If the drop message action is executed in a embedded Tuxedo call, the whole call fails.

1.2.7.1.1.2 Tuxedo Components

The Component Scope panel contains the following selections:

- Domain Group: For service statistics alerts only.
- Domain: Optional
- Machine: Optional
- Group: Optional
- Server: Optional

> **Note**
>
> Machine, Group, and Server can also accept FML32 boolean expressions.

Click the radio button to select input method (use the drop-down list or manually enter an FML32 boolean expression). The values of each level is determined by its parent level, except for Domain.

- Services: For service statistics alerts only.

1.2.7.1.1.3 Metrics Evaluation Expression(s)

You can select the metric, operator and threshold to compose one expression. The logic for the expression can be "and" or "or".

1.2.7.1.1.4 FML Boolean Expression(s)

You can also input FML Boolean expressions directly. For more information, see Alert Metrics Tables. For call path alerts, if the elapsed time *only* is evaluated in the evaluation expression, the alert is triggered once along the entire call path. Other metrics combined with elapse time do not have this effect.

> **Note**
>
> The TSAM Plus Console cannot guarantee FML Boolean expression syntax correctness.

1.2.7.1.2 Adaptive Settings (For Service Statistics Alerts Only)

For service statistics alerts, when you select Adaptive Threshold in the Logic for Expression panel, you need to continue to configure the Adaptive Settings. It specifies a past time of which the metrics data are used for comparison with current time collected data. If the comparison result meets the criteria you set in the metrics evaluation expression, an alert is reported.

- **Daily**: the average or aggregated metrics data of one day is compared for evaluation. You can select one day of the past 30 days.
- **Hourly**: the average or aggregated metrics data in one hour of a day is compared for evaluation. You can specify how many hours ahead (-) of or after (+) current hour in one day of the past 30 days.
  For example, if you define an adaptive alert evaluation expression for the response time metrics and specify **Adaptive Settngs** as “Hourly, 1 day ago,-5 hours”, the average response time between 1:00 pm to 2:00 pm yesterday will be used for comparison with each response time data collected during 6:00-7:00 pm today.

  The **Per Service Instance** is only available for the time-related metrics, of which average data is calculated. When this option is checked, the metrics data collected from each service instance is evaluated against the historical average data.

1.2.7.2 CICS Alert Definition

Click **Alert** and select **CICS Alert Definition** from the drop-down list; the **CICS Alert Definition List** panel appears. This panel lists available CICS alert definitions and allows you to create, edit, and manage alert definitions.

- CICS Alert Definition List Panel
- Define New Alert Panel

1.2.7.2.1 CICS Alert Definition List Panel

The following tables list the **CICS Alert Definition List** menu bar options and columns respectively.

Table 1-61 CICS Alert Definition List Menu Bar

Elements	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns to shown in the table • Detach: Displays the table in a separate window • Sort: Sort the table • Reorder Columns: Change the order how the columns are displayed
Add	Creates a new alert definition.
Delete	Deletes the alert definition.
Enable	Enables the alert definition.
Disable	Disables the alert definition.

Table 1-61 (Cont.) CICS Alert Definition List Menu Bar

Elements	Description
Edit	Modifies the alert definition.
Clone	Creates a new alert with same definition as current alert but the name is left empty.
Alerts	Identifies all alerts generated by this alert definition.
Refresh	Updates the alert definition list.
Detach	Displays the table in a separate window.

Table 1-62 Alert Definition List Columns

Column	Description
Selection checkbooks	Select a set of alert definitions in current page for processing.
Name	The alert name which is specified in alert definition
Status	Displays alert status. The status could be enabled or disabled. • Enable: The alert definition enabling request has been sent to Tuxedo. • Disable: The alert definition disabling request has been sent to Tuxedo.
Type	The monitoring category and system, consistent with policy definition. The category types are as follows: • CICS Transaction • CICS Terminal
Evaluation Condition	The FML Boolean expression of the alert triggering conditions.

1.2.7.2.2 Define New Alert Panel

Click **Add** or **Clone** on the menu bar; the **Define New Alert** panel appears. This panel allows you to define concrete Tuxedo Application Runtime alert definitions.

The Define New Alert panel is divided into three sections:

- Alert Properties
- Metrics Evaluation Expression(s)
- FML Boolean Expression(s)

1.2.7.2.2.1 Alert Properties

The following table lists the **Alert Properties** options.

Table 1-63 Alert Properties Options

Column	Description
Name	The name of the alert. It must be unique among the alerts globally. The name value is limited to 255 characters and must be unique within the project. The initial character must not be a "."
CICS Region	Defines the function scope of the defined alert.
Type	The type of the alert; it is based on monitoring policy. The drop-down list includes the following items: • CICS Transaction • CICS Terminals

Table 1-63 (Cont.) Alert Properties Options

Column	Description
Severity	The severity drop-down list contains the following: • Fatal • Critical • Warn • Information
Interval	It accepts an integer value (in seconds). The current alert is evaluated only once during this interval. The purpose is to throttle alert volume in a similar scenario.
Action	Specifies what kind of action is executed when an alert definition set to "true". It supports the following action: • Publish to Tuxedo Event Broker An event is posted to the Oracle Tuxedo event broker. The event name is the alert name by default; you can also specify it manually. The buffer is an FML32 buffer containing the metric snapshot.

1.2.7.2.2.2 Metrics Evaluation Expression(s)

You can select the metric, operator and threshold to compose one expression. The logic for the expression can be "`and`" or "`or`".

1.2.7.2.2.3 FML Boolean Expression(s)

You can also input FML Boolean expressions directly. For more information, see Alert Metrics Tables.

> **Note**
>
> The TSAM Plus Console cannot guarantee FML Boolean expression syntax correctness.

1.2.7.3 IMS Alert Definition

Click **Alert** and select **IMS Alert Definition** from the drop-down list; the **Alert Definition List** panel appears. This panel lists available Tuxedo Application Runtime IMS alert definitions and allows you to create, edit, and manage alert definitions.

- IMS Alert Definition List Panel
- Define New Alert Panel

1.2.7.3.1 IMS Alert Definition List Panel

The following tables list the **IMS Alert Definition List** menu bar options and columns respectively.

Table 1-64 IMS Alert Definition List Menu Bar

Elements	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns to shown in the table • Detach: Displays the table in a separate window • Sort: Sort the table • Reorder Columns: Change the order how the columns are displayed
Add	Creates a new alert definition.
Delete	Deletes the alert definition.
Enable	Enables the alert definition.
Disable	Disables the alert definition.
Edit	Modifies the alert definition.
Clone	Creates a new alert with same definition as current alert but the name is left empty.
Alerts	Identifies all alerts generated by this alert definition.
Refresh	Updates the alert definition list.
Detach	Displays the table in a separate window.

Table 1-65 Alert Definition List Columns

Column	Description
Selection checkbooks	Select a set of alert definitions in current page for processing.
Name	The alert name which is specified in alert definition
Status	Displays alert status. The status could be enabled or disabled. Enable: The alert definition enabling request has been sent to Tuxedo. Disable: The alert definition disabling request has been sent to Tuxedo.
Type	The monitoring category and system, consistent with policy definition. The category types are as follows: • IMS Transaction • IMS Program
Evaluation Condition	The FML Boolean expression of the alert triggering conditions.

1.2.7.3.2 Define New Alert Panel

Click **Add** or **Clone** on the menu bar; the **Define New Alert** panel appears. This panel allows you to define concrete Tuxedo Application Runtime IMS alert definitions.

The Define New Alert panel is divided into three sections:

- Alert Properties
- Metrics Evaluation Expression(s)
- FML Boolean Expression(s)

1.2.7.3.2.1 Alert Properties

The following table lists the **Alert Properties** options.

Table 1-66 Alert Properties Options

Option	Description
Name	The name of the alert. It must be unique among the alerts globally. The name value is limited to 255 characters and must be unique within the project. The initial character must not be a "."
Domain	Defines the function scope of the defined alert.
Type	The type of the alert; it is based on monitoring policy. The drop-down list includes the following items: • IMS Transaction • IMS Program
Severity	The severity drop-down list contains the following: • Fatal • Critical • Warn • Information
Interval	It accepts an integer value (in seconds). The current alert is evaluated only once during this interval. The purpose is to throttle alert volume in a similar scenario.
Action	Specifies what kind of action is executed when an alert definition set to "true". It supports the following action: • Publish to Tuxedo Event Broker An event is posted to the Oracle Tuxedo event broker. The event name is the alert name by default; you can also specify it manually. The buffer is an FML32 buffer containing the metric snapshot.

1.2.7.3.2.2 Metrics Evaluation Expression(s)

You can select the metric, operator and threshold to compose one expression. The logic for the expression can be "`And`" or "`Or`".

1.2.7.3.2.3 FML Boolean Expression(s)

You can also input FML Boolean expressions directly. For more information, see Alert Metrics Tables.

1.2.7.4 Batch Alert Definition

You can view, add, edit and delete JES Alert Definitions through Alert Definition

Click **Alert** and select **Batch Alert Definition** from the drop-down list; the **Batch Alert Definition List** panel appears. This panel lists available Batch alert definitions and allows you to create, edit, and manage alert definitions.

- Batch Alert Definition List Panel
- Batch Alert Definition Filter Conditions
- Batch Alert Definition Details

1.2.7.4.1 Batch Alert Definition List Panel

The following table list the **Batch Alert Definition List** menu bar options and columns respectively.

Table 1-67 Batch Alert Definition List Menu Bar

Elements	Description
View	From the drop-down menu, you can select the following: • Columns: Select the columns to shown in the table • Detach: Displays the table in a separate window • Sort: Sort the table • Reorder Columns: Change the order how the columns are displayed
Add	Creates a new alert definition.
Delete	Deletes the alert definition.
Enable	Enables the alert definition.
Disable	Disables the alert definition.
Edit	Modifies the alert definition.
Clone	Creates a new alert with same definition as current alert but the name is left empty.
Alerts	Identifies all alerts generated by this alert definition.
Refresh	Updates the alert definition list.
Detach	Displays the table in a separate window.

Click **Add** or **Edit**; the **JES Alert Definition panel** appears.

Table 1-68 Alert Properties Options

Elements	Description
Name	The name of the alert. It must be unique among the alerts globally. The name value is limited to 255 characters and must be unique within the project. The initial character must not be a .
Type	The type of the alert; it is based on monitoring policy. The drop-down list includes the following items: • JES Jobs • JES Metrics
Severity	The severity drop-down list contains the following: • Fatal • Critical • Warn • Information
Interval	It accepts an integer value (in seconds). The current alert is evaluated only once during this interval. The purpose is to throttle alert volume in a similar scenario.

1.2.7.4.2 Batch Alert Definition Filter Conditions

The following table lists the **Batch Alert Definition Filter Conditions** options.

Table 1-69 Batch Alert By Filter Options

Options	Description
JES Application	Identifies which JES application the Job is executed, single choice drop-down list, required. **Note** Job information can be only be obtained when the selected JES application is alive. If an inactive JES application is selected when clicking the 'Query' button, a warning message window is displayed.
Job Name	The string contained in the job name, input text box.
Job Owner	One or more owners of the job, input text box.
Job Priority	One or more priorities.
Job Class	The job class, multiple choice drop-down list.

1.2.7.4.3 Batch Alert Definition Details

If the **Type** is Batch Job, the Batch metric detail panel provides the information shown in the tables below. Three levels of metric details can be selected and displayed: Job Status, Job Execution Time, and Job.

Table 1-70 JES Job Type Detailed Information

Elements	Description
Job Status	Job status is changed to the specified status. You can specify one of the following: • EXECUTING • CONVING • WAITING • DONE • FAIL • HOLD_WAITING • HOLD_CONVING • INDOUBT • DISCARD
Job	Job is purged
Job Execution Time	Job execution time >= ? millisecond during the last Interval seconds

If the **Job Type** is JES Metrics, the JES metric detail panel provides the information shown in table below:

Table 1-71 JES Metrics Type Detailed Metrics

Elements	Description
Jobs average execution time	Job average execution time >= ? millisecond during the last Interval seconds
Jobs fails number	Jobs fails number >= during the last Interval seconds
Jobs waiting number	Jobs waiting number >= during the last Interval seconds

1.2.7.5 Alert Query

Alert Query view displays the alerts that have transpired. It includes metric alerts and system alerts. Metrics alert are the events generated against the defined metrics alert. System alerts represent system events.

Click **Alerts** and select **Alert Query** from the drop-down menu; the **Alert Query** page appears. The Alert Query page contains two tabs:

- Unread Alerts Tab
- Historical Alerts Tab

1.2.7.5.1 Unread Alerts Tab

"Unread" alerts are most important for administrators because they represent events that they may not be aware of. The Unread Alerts tab contains two sections:

- Filtering Condition
- Unread Alert Columns

The following table lists the **Alert Query** filtering condition options.

Table 1-72 Alert Query Filtering Conditions

Options	Description
Contains	Select a set of alerts in current page for processing.
Type	The monitoring category and system are consistent with policy definition. The following category types are as follows: • Any • Call Path • Service • Service Statistics • XA Transaction • BRIDGE • GWTDOMAIN • GWWS • CICS Transaction • CICS Terminals • JES Job • JES Metrics • IMS Transaction • IMS Program • System **Note** System represents this is a system-level event generated by Oracle TSAM Plus

Table 1-72 (Cont.) Alert Query Filtering Conditions

Options	Description
Severity	Four severity levels are supported: • Any • Fatal • Critical • Warn • Information

The following table lists the Alert Query columns.

Table 1-73 Alert Query Columns

Column	Description
Selection checkbox	Select a set of alerts in current page for processing.
Name	The alert name which is specified in alert definition.
Type	The monitoring category and system are consistent with policy definition. The following category types are as follows: • Any • Call Path • Service • Service Statistics • XA Transaction • BRIDGE • GWTDOMAIN • GWWS • CICS Transaction (Tuxedo Application Runtime only) • CICS Terminals (Tuxedo Application Runtime only) • IMS Transaction • IMS Program • JES Job (Tuxedo Application Runtime only) • JES Metrics (Tuxedo Application Runtime only) • System **Note** System represents this is a system-level event generated by Oracle TSAM Plus.
Severity	Four severity levels are supported: • Any • Fatal • Critical • Warn • Information
Cleared	Indicates whether the alert has been marked as read.
Clear Time	Identifies the time an alert is “cleared.”
Log Time	The time an Alert occurs.

Table 1-73 (Cont.) Alert Query Columns

Column	Description
Description	The reason/cause for the alert. It uses the following format: `"Process [%s:%d] evaluates alert [%s] with true, metrics[key=value,key=value...]"`

Click **Clear** to clear all the selected alerts on current page.

Click **Delete** to delete all the selected events on current page.

Click **Detail**, a pop-up window with the following detailed Alert information appears:

- All information in the alerts summary data grid.
- The metrics detail and reason string for this alerts.
  Once an alert is cleared as "Unread" status and not deleted, it still can be queried in the historical alert page, but not in the active alert page. The following filter conditions can be set:
  - Alert Type
  - Alert Severity
  - A custom "search" text string

  The search operation finds matched records from all current filtered "unread" alert results, no limited to the "unread" alerts shown on the current page. Matched record means any alert that is matching the specified alert category condition, alert severity condition and having the given "search" text string within any of the following value fields: "Alert Name", "Alert Reason String (Description)".

Click the **Reset** button to reset filter conditions and list all "unread" alerts.

1.2.7.5.2 Historical Alerts Tab

The Historical Alerts Tab allows you to query historical alerts with supplied filtering conditions. It contains two panels:

- Historical Alert Query Conditions
- Alerts Query Results

The following table lists the **Historical Alert Query Conditions** panel options.

Table 1-74 Historical Alerts Query Conditions Options

Options	Description
Alert Name	The Alerts names configured in this project. "Any" is a reserved key word meaning all alerts.
Type	"Any" and the supported monitoring categories. System is in same level with other monitoring categories.
Severity	"Any" and supported severity levels. If is checked, all alerts at this level or below are queried. The sequence is Fatal, Critical, Warn and Info.
Query During	The exact time of the previous day to the exact time of the current day. For example: 7:45 Wednesday-to-7:45 Thursday.

Click **Submit**; the results are displayed in the **Alert Query Result** panel.

1.2.7.6 System Alerts Supported

Users cannot define System Alerts; they are generated automatically (for example, an invalid alert definition is encountered, or the database purging process is completed).

The following table lists the supported system alerts.

Table 1-75 System Alerts Supported

Alert name	Alert Severity	Alert Reason String
.INVALIDEXP	warning	Alert definition [%ALERT_NAME] has invalid evaluation expression
DB.PURGE	information	Data purging sequence:?) filed at [%DATE_TIME] by admin is done.

1.2.7.7 Alert Metrics Tables

The Alert Metrics tables contain the alert metrics for all alert types. Each metric has the corresponding FML32 field name and applicable operators. Referencing these tables will help you write the alert metric FML boolean expression directly when defining a new alert.

- Call Path Alert Metrics Table
- Service Alert Metrics Table
- GWTDOMAIN/BRIDGE Alert Metrics Table
- GWWS Alert Metrics Table
- XA Transaction Alert Metrics Table
- CICS Transaction Alert Metrics Table
- CICS Terminals Alert Metrics Table
- IMS Transaction Alert Metrics Table
- IMS Program Alert Metrics Table

1.2.7.7.1 Call Path Alert Metrics Table

Table 1-76 Call Path Alert Metrics Table

Metric	FML32 Field	Operators
Elapse Time	TA_MONELAPSETIME	>, >=
Execution Status	TA_MONERRNO	==, !=
URcode	TA_MONURCODE	==, !=
Depth	TA_MONDEPTH	>, ==, <
Message Number on Request Queue	TA_MONMSGQUEUED	>, >=

1.2.7.7.2 Service Alert Metrics Table

Table 1-77 Service Alert Metrics Table

Metric	FML32 Field	Operators
Execution Time	TA_MONEXECTIME	>, >=
Execution Status	TA_MONERRNO	==, !=
Request Message Size	TA_MONMSGSIZE	>, >=
Message Number on Request Queue	TA_MONMSGQUEUED	>, >=
URcode	TA_MONURCODE	==, !=
Waiting Time	TA_MONMSGWAITTIME	>, >=
CPU Time	TA_MONCPUTIME	>, >=

1.2.7.7.3 GWTDOMAIN/BRIDGE Alert Metrics Table

Table 1-78 GWTDOMAIN/BRIDGE Alert Metrics Table

Metric	FML32 Field	Operators
Link Status (GWTDOMAIN/ BRIDGE)	TA_MONLINKSTATUS	Lost, Reconnect
Outstanding Request (GWTDOMAIN)	TA_MONNUMWAITRPLY	>, >=

1.2.7.7.4 GWWS Alert Metrics Table

Table 1-79 GWWS Alert Metrics Table

Metric	FML32 Field	Operators
Inbound one way failed number	TA_MONINOWFAIL	>, >=
Outbound one way failed number	TA_MONOUTOWFAIL	>, >=
Inbound RPC failed number	TA_MONINRPCFAIL	>, >=
Outbound RPC failed number	TA_MONOUTRPCFAIL	>, >=
Inbound average processing time	TA_MONINTIME	>, >=
Outbound average processing time	TA_MONOUTTIME	>, >=
Inbound Pending Request	TA_MONINBOUNDPEND	>=
Outbound Pending Request	TA_MONOUTBOUNDPEND	>=

1.2.7.7.5 XA Transaction Alert Metrics Table

Table 1-80 XA Transaction Alert Metrics Table

Metric	FML32 Boolean Expression
Transaction Failed	TA_MONXANAME=='tpabort' || TA_MONXANAME=='xa_rollback'
Heuristically Completed	TA_MONXANAME=='xa_commit' && TA_MONXACODE==8

Table 1-80 (Cont.) XA Transaction Alert Metrics Table

Metric	FML32 Boolean Expression
Heuristically Commit	TA_MONXANAME=='xa_commit' && TA_MONXACODE==7
Resource Manager Failure	TA_MONXANAME%%'xa_.* ' && TA_MONXACODE==-3

1.2.7.7.6 CICS Transaction Alert Metrics Table

Table 1-81 CICS Transaction Alert Metrics Table

Metric	FML32 Field	Operators
Execution Time	TA_MONEXECTIME	>, >=
Message Number on Request Queue	TA_MONMSGQUEUED	>, >=
Waiting Time	TA_MONMSGWAITTIME	>, >=
CPU Time	TA_MONCPUTIME	>, >=

1.2.7.7.7 CICS Terminals Alert Metrics Table

Table 1-82 CICS Terminals Alert Metrics Table

Metric	FML32 Field	Operators
Average Session Number	TA_MONSESSIONNUM	>, >=
Number of CICS Transactions Failed	TA_MONTRANFAIL	>, >=

1.2.7.7.8 IMS Transaction Alert Metrics Table

Table 1-83 IMS Transaction Alert Metrics Table

Metric	FML32 Field	Operators
Execution Time	TA_IMS_EXECUSEC	>, >=
CPU Time	TA_IMS_CPUTIMEUSEC	>, >=
DLI Time	TA_IMS_DLIUSEC	>, >=

1.2.7.7.9 IMS Program Alert Metrics Table

Table 1-84 IMS Program Alert Metrics Table

Metric	FML32 Field	Operators
Execution Time	TA_IMS_EXECUSEC	>, >=
CPU Time	TA_IMS_CPUTIMEUSEC	>, >=
DLI Time	TA_IMS_DLIUSEC	>, >=

1.3 Oracle TSAM Plus Group/User Privileges

The following table lists the Oracle TSAM Plus Group/User privilege options.

Table 1-85 Oracle TSAM Plus Group/User Privileges

Category	Privilege(s)
User Management	view, administrate
Group Management	view, administrate.
Data Management	administrate
Tuxedo Component Tree	view, administrate
ART region Tree	view, administrate
JES Component Tree	view, administrate
Global Parameter Setting	view, administrate
Tuxedo Policy Definition	view, administrate
ART Policy Definition	view, administrate
Tuxedo Alert Definition	view, administrate
ART alert Definition	view, administrate
Tuxedo Alert	view, administrate
ART Alert	view, administrate
Tuxedo Metrics	view Service Metrics, view call path Metrics, view transaction Metrics, view gateway Metrics, view bridge Metrics, view GWWS Metrics
ART Metrics	View Terminal Metrics, view CICS transaction Metrics
JES Metrics Management	View JES Metrics, administrate

Note

- For lower left **Unread Alert** notification panel:
  - If you have Tuxedo Alert view privilege, but do not have ART alert view privilege, only the numbers of the Tuxedo alerts are shown.
  - If you do not have Tuxedo alert view privilege, but have ART alert view privilege, only the numbers of the ART alerts are shown.
  - If you do not have both Tuxedo and ART alert view privileges, the entire panel is hidden.
- On the alert query page, if you have both Tuxedo alert view and ART alert view privileges, both types of alerts can shown in the query result table. However, without corresponding administrate privilege, administrator tasks (such as **Clear** and **Delete**) are not available.
  For example, you have Tuxedo alert, ART alert and Tuxedo alert administrate privileges. When you select all the queried out alerts (including both Tuxedo alert and ART alert type), the **Clear** and **Delete** button above the query result table is disabled.
- Group privilege is based on the User View privilege. The user cannot enter the group management console without User Management view privileges.

1.4 AI Operations Assistant

This section contains the following topics:

- Overview
- AI Setup Prerequisites
- Features of the TSAM Operations Assistant
- Accessing the TSAM Operations Assistant
- Using the Operations Assistant
- Configuring the Operations Assistant
- Sample Questions

1.4.1 Overview

Oracle TSAM Plus 22c onwards, an AI-based Operations Assistant is now available. The Operations Assistant performs the following functions:

- Answers questions about how to use Oracle TSAM Plus
- Answers questions related to the configuration and metrics data for the Tuxedo domains that Oracle TSAM Plus is monitoring

You can interact with the AI-based Operations Assistant by typing natural-language requests. Initial suggestions and follow-up suggestions may also appear when settings options are enabled.

1.4.2 AI Setup Prerequisites

> **Note**
>
> The Operations Assistant is available only after TSAM Plus AI setup is completed, including enabling AI deployment, configuring the TSAM Plus AI database user, provider/model/credential settings, and creating the required Select AI credentials/ profiles/agent metadata. If this setup is incomplete, the console readiness check keeps the assistant unavailable.

1.4.3 Features of the TSAM Operations Assistant

Following is a list of features of the TSAM 22c Operations Assistant:

- **Initial Suggestions**
  When enabled in Settings, the Operations Assistant shows starter suggestions for a new chat.
- **Ask Questions**
  Type a request in the message input and send it to the Operations Assistant. The assistant displays the response in the conversation.
- **Follow-up Suggestions**

When enabled in Settings, completed responses can show follow-up suggestions. Selecting one fills the message input for review or editing before sending.

- **Conversations**
  TSAM Plus stores conversations for the current user in Recent and Archived views. Each view separates pinned conversations from the normal list. A user can pin up to 20 conversations total; pinned conversations are ordered within their current Recent or Archived view. Search applies only to the selected view that matches conversation titles and recent questions. Show more conversations loads normal rows. Users can reopen conversations and manage them by pinning, unpinning, reordering pinned conversations with drag or Move up/Move down, renaming, marking as read or unread, exporting JSON, archiving, restoring, or deleting them. Archived conversations remain writable until deleted; restoring moves them to Recent.
- **Configuration**
  Users can configure Operations Assistant settings and view or update the AI profile configuration. For more information, see Configuring the Operations Assistant.
- **Providing Feedback**
  For completed responses, use thumbs up or thumbs down to mark the answer as helpful or not helpful. Select the other option to change feedback, or select the same option again to remove it.
- **Generated SQL**
  When generated SQL is available for a response, a <SQL> icon appears with the response. Click the icon to display the generated SQL, select Copy SQL to copy it, or select the icon again to hide it. The generated SQL is also included when the conversation is exported as JSON.
- **Copy**
  Users can copy questions and responses when copy support is available in the browser.

1.4.4 Accessing the TSAM Operations Assistant

On the Main Page of Oracle TSAM Plus Console, click **Show Operations Assistant** to open the Operations Assistant. If the current browser session has saved the assistant pane as visible, the console performs a readiness check and restores the pane when the check succeeds. If the check fails, the pane remains closed. The button remains unpressed, and an unavailable message offers **Retry readiness check**.

Click **New Chat** to start a blank chat. A server-side conversation is created only after the first request is sent. Existing conversations persist in the Conversations panel; reopening one makes it active and writable. Click **Hide Operations Assistant** at the top right to hide the pane without deleting the active conversation.

1.4.5 Using the Operations Assistant

Use the message input to ask the Operations Assistant. If suggestions are enabled, select an initial or follow-up suggestion. Click **Send** or press **Enter** to submit.

Ask Questions

For long-running responses, the assistant polls for up to 120 seconds in the foreground. If a response is pending, users cannot submit another question in the same conversation, and they can cancel pending responses if that action is available. In case the response times out before completion, click **Resume** for another 120-second foreground polling round to continue checking.

Starting a New Chat

Click **New Chat** in the Conversations panel to clear the chat view. A server-side conversation is created only after the first request is sent.

Managing Conversations

In Managing Conversations, you can mark a conversation as read or unread. You can export a single conversation from the row-level Export JSON action, or export the active conversation from **Menu > Export**. **Open Menu > Conversations**. Recent and Archived show current-user conversations in separate views, each with pinned (up to 20) and normal sections. Search stays within the selected view; Show more conversations loads normal rows. Click a conversation to make it active and writable. From its row action menu, pin/unpin, rename, export JSON, archive/restore, or delete. Reorder pinned conversations by dragging or using Move up/Move down. Delete requires confirmation. Use Collapse conversations or Back to chat to return to the chat view. Use **Show more conversations** to load earlier messages in the active conversation. If users try to close **Settings** with unsaved changes, the assistant prompts them to save or revert the changes first.

Providing Feedback

For completed responses, use thumbs up or thumbs down to mark the answer as helpful or not helpful. Select the other option to change feedback, or select the same option again to remove it.

1.4.6 Configuring the Operations Assistant

You can configure the Operations Assistant by using the following menu items:

Settings

Open Settings to configure the following options:

- Enable or disable follow-up suggestions.
- Enable or disable initial suggestions
- Set the number of conversations displayed per page to 10, 20, or 50. The default is 20.
- Automatically delete unpinned conversations after 30, 90, or 365 days, or select Never to retain them indefinitely. The default is 365 days. Pinned conversations are not deleted automatically. Automatic cleanup applies to them only after they are unpinned.
- Enable or disable knowledge-based retrieval for questions about how to use Oracle TSAM Plus. When enabled, the Operations Assistant grounds its responses in the prepared TSAM Plus knowledge base. The option is disabled by default. With less capable LLM models, enabling this option can improve response quality.
- Set the response length and level of detail to **Brief**, **Standard**, or **Elaborate**. The default is **Standard**.

AI Profile Configuration

Open **AI Profile Configuration** to view and/ or edit the current AI profile configuration.

The configuration includes the AI provider, and the parameters used by the provider. The parameters can include:

- Model: The LLM model used by the Operations Assistant.
- Max tokens: The maximum number of tokens that the model can generate.

When the provider is OCI, you can modify Model and Max tokens and click **Save** button to save the changes.

Note: Saved changes are applied to all AI profiles.

Click **Refresh** button to reload the current AI profile definition.

1.4.7 Sample Questions

Open **Sample Questions** to view example questions for common Operations Assistant use cases. The questions are organized by themes. Click a question to copy it to the message input, where you can review and/ or edit it before sending.

2

Oracle Tuxedo Scripting Tool

This chapter describes the Oracle Tuxedo Scripting Tool (TXST). It explains how you use the TXST command-line scripting interface to configure, manage, and persist change to Tuxedo running instances and monitor and manage server run-time events.

This chapter is organized as follows:

- Using the Tuxedo Scripting Tool describes how the scripting tool works, its modes of operation, and the basic steps for invoking it.
- Navigating MBeans describes how to retrieve Tuxedo domain configuration and run-time information, and edit configuration or custom MBeans.
- Managing the Server Life Cycle describes using TXST to start and stop Tuxedo Server instances and to monitor and manage the server life cycle.

- Using the Tuxedo Scripting Tool
- Navigating MBeans
- Managing the Server Life Cycle

2.1 Using the Tuxedo Scripting Tool

This chapter contains the following topics:

- What is the Tuxedo Scripting Tool?
- Modes of Operation
- Main Steps for Using TXST

2.1.1 What is the Tuxedo Scripting Tool?

The Tuxedo Scripting Tool (TXST) is a command-line scripting environment that you can use to manage, and monitor Tuxedo domains. The TXST scripting environment is based on the Java scripting interpreter, Jython. In addition to supporting standard Jython features such as local variables, conditional variables, and flow control statements, TXST provides a set of scripting functions (commands) that are specific to Tuxedo. See http://www.jython.org.

- How Does TXST Work?

2.1.1.1 How Does TXST Work?

You can use the scripting tool online (connected to a running Tuxedo domain or a JMX agent embedded in the tlisten process). For information on TXST commands, see TXST Command and Variable ReferenceTXST Command and Variable Reference.

Online, TXST provides simplified access to Managed Beans (MBeans), Java objects that provide a management interface for an underlying resource that you can manage through JMX.

When TXST is connected to a Tuxedo domain, the scripting tool lets you navigate and interrogate MBeans, and supply configuration data to the instance. When TXST is connected to a JMX agent, its functionality is limited to commands which MBeans support.

2.1.2 Modes of Operation

TXST is a command-line interpreter that interprets commands either interactively, supplied one-at-a-time from a command prompt, or in batches, supplied in a file (script), or embedded in your Java code. The modes of operation represent methods for issuing TXST commands:

- Interactively, on the command line—Interactive Mode
- In a text file—Script Mode
- Embedded in Java code—Embedded Mode

- Interactive Mode
- Script Mode
- Embedded Mode

2.1.2.1 Interactive Mode

Interactive mode, in which you enter a command and view the response at a command-line prompt, is useful for learning the tool, prototyping command syntax, and verifying configuration options before building a script. Using TXST interactively is particularly useful for getting immediate feedback after making a critical configuration change. The TXST scripting shell maintains a persistent connection with an instance of Tuxedo domain. Because a persistent connection is maintained throughout the user session, you can capture multiple steps that are performed against the instance. For more information, see Recording User Interactions.

2.1.2.2 Script Mode

Scripts invoke a sequence of TXST commands without requiring your input, much like a shell script. Scripts contain TXST commands in a text file with a .py file extension, for example, filename.py. You use script files with three modes(Invoking TXST with the script, using Jython commands for running scripts and invoking the script with Ant build file). See Running Scripts.

2.1.2.3 Embedded Mode

In embedded mode, you instantiate an instance of the TXST interpreter in your Java code and use it to run TXST commands and scripts. Except for `startRecording()` and `stopRecording()`, all TXST commands and variables that you use in interactive and script mode can be run in embedded mode.

The following code snippet illustrates how to instantiate an instance of the TXST interpreter and use it to connect to a running domain and create a server.

Running TXST From a Java Class

```
import java.util.*;
import oracle.tuxedo.jmx.tux.jyscript.TXSTInterpreter;
import org.python.util.InteractiveInterpreter;

public class EmbeddedTXST {
  static InteractiveInterpreter interp = null;
```

```
  EmbeddedTXST() {
    interp = new TXSTInterpreter();
  }
  private static void connect() {
    interp.exec("connect('//localhost:5037', 'simpapp', ‘38075’)");
  }
  private static void create_server() {
    StringBuffer buffer = new StringBuffer();
    buffer.append("cd('simple/GROUP1')\n");
    buffer.append("srv1= create(‘simpserv’, ‘SERVER’, srvID=40)\n");
    buffer.append("print 'Script ran successfully...'\n");
    interp.exec(buffer.toString());
  }
  public static void main(String[] args) {
    new EmbeddedTXST();
    connect();
    create_server();
  }
}
```

2.1.3 Main Steps for Using TXST

The following sections summarize the steps for setting up and using TXST:

- Setting Up Your Environment
- Invoking TXST
- Requirements for Entering TXST Commands
- Running Scripts
- Exiting TXST
- Getting Help
- Recording User Interactions
- Redirecting TXST Output to a File

2.1.3.1 Setting Up Your Environment

To set up your environment for TXST:

1. Install and configure the TSAM Plus agent.
2. Set `TUXDIR` environment variable as Tuxedo install directory and `$TUXDIR/bin` to the PATH environment variable.
3. Include `$TUXDIR/jmx/jython-standalone.jar:$TUXDIR/jmx/tmjmx_tux.jar:$TUXDIR/jmx/tmjmx_metadata.jar` in the `CLASSPATH`. Or you can invoke TXST just using `txst.sh` or `txst.cmd` which we provided.

2.1.3.2 Invoking TXST

To invoke TXST, enter the following command: **txst.sh**

A welcome message and the TXST prompt appears:

```
txst: /offline>
```

txst.sh is placed in $TUXDIR/bin. If you invoke TXST with txst.sh, you do not need to set up the CLASSPATH.

If you added the related jar files into CLASSPATH as we mentioned before, you can enter the command: java oracle.tuxedo.TXST. For instance,

```
#export CLASSPATH=$CLASSPATH:$TUXDIR/jmx/jython-standalone.jar:$TUXDIR/jmx/
tmjmx_tux.jar:$TUXDIR/jmx/tmjmx_metadata.jar
#java oracle.tuxedo.TXST
Initializing Tuxedo Scripting Tool (TXST) ...
```

> **Note**
>
> If using dmib related commands, you should use the package $TUXDIR/udataobj/tuxj/com.bea.core.jatmi_2.0.0.0.jar

Jython scans all the jar files it can find at first startup. Depending on the system, this process may take a few minutes to complete, and TXST may not return a prompt right away.

```
Welcome to Tuxedo Administration Scripting Tool
Type help() for help on available commands
txst:/offline>
```

2.1.3.3 Requirements for Entering TXST Commands

Follow these rules when entering TXST commands. Also see TXST Command and Variable Reference.

- Command names and arguments are case sensitive.
- Enclose arguments in single or double quotes. For example, 'newServer' or "newServer".
- If you specify a backslash character (\) in a string, for example when specifying a file pathname, you should precede the quoted string by r to instruct TXST to interpret the string in its raw form and ensure that the backslash is taken literally. This format represents standard Jython syntax.
- Display help information for TXST commands by printing the command's documentation string. See Getting Help.

2.1.3.4 Running Scripts

TXST incorporates three ways for running scripts. To run the script examples in this guide, copy and save the commands in a text file with a .py file extension, for example, filename.py. Use the text file with the commands for running scripts that are listed below. There are sample scripts that you can use as a template when creating a script.py file from scratch. If the script will connect TXST to a running Tuxedo domain, start Tuxedo domain before running the script.

You can run the script in three modes:

- Invoke TXST and run a script:
  `java oracle.tuxedo.TXST myscript.py`
- run a script from TXST:

```
execfile('myscript.py')
```

Listing 2-2 Running script myscript.py

```
connect("//localhost:5037", "simpapp", "38075");
cd('simple/GROUP1')
ls('c')
disconnect()
exit()
```

- Invoke the TXST script from an Ant build file
  Scripts invoke a sequence of TXST commands without requiring your input, much like a shell script. Scripts contain TXST commands in a text file with a .py file extension.

  TXST provides a custom ant task to invoke the TXST script from an Ant build file. If you want to use the task with your own Ant installation,add the following task definition in your build file:

  ```
  <taskdef name ="txst" classname="oracle.tuxedo.jmx.tux.jyscript.TXSTTask"/>
  ```

- To run TXST from an Ant script:
  - Set your environment in a command shell,which include `TUXDIR`,`CLASSPATH`,`JAVA_HOME`,`ANT_HOME` and so on.
  - Add a call to the txst Ant task to execute TXST commands. For example:

    ```
    <target name="GetParameters">
      <txst debug="false" failOnError="false"
    executeScriptBeforeFile="true" fileName="./test.py">
        <script>
          connect("//slce04cn03:5067","simpapp","38175")
          ls()
          print cmo.GetParameters()
        </script>
      </txst>
    </target>
    ```

    Using the txst Ant task, you can specify TXST commands within a TXST script(.py), using the fileName attribute, or embed TXST script commands inside the build file, within the <script> tags.
  - Execute the Ant task or tasks specified in the build.xml file by typing ant in the staging directory, optionally passing the command a target argument:
    ```
    bash-3.2$ ant getParameters
    ```
  - the syntax of the txst Ant task is as follows:
    ```
    <txst properties="propsFile" filename=”filename” arguments="arglist"
    failOnError=”value” executeScriptBeforeFile="value” debug=”value” >

    <script>

    txst-commands

    </script>
    ```

The following table defines the Ant task attributes that you can specify as part of the txst Ant task.

Table 2-1 Ant Task Attributes

Attribute	Definition
`properties="propsFile"`	Optional. Name and location of the properties file that contains name-value pairs that you can reference in your script.
`fileName="fileName"`	Optional. Name and location of the TXST script file that you would like to execute. If the specified TXST script file does not exist, the txst Ant task fails.
`arguments="arglist"`	Optional. List of arguments to pass to the script. These arguments are accessible using the sys.argv variable.
`failOnError="value"`	Optional. Boolean value specifying whether the Ant build script will fail if the txst Ant task fails. This attribute defaults to true.
`executeScriptBeforeFile="value"`	Optional. Boolean value specifying whether the embedded script is executed before the specified TXST script file. This attribute defaults to true, specifying that the embedded script is executed first.
`debug="value"`	Optional. Boolean value specifying whether debug statements should be output when the TXST Ant Task is executed. This attribute defaults to false.

In the following example, test.py is the file in which there are TXST commands. You also can add TXST command in the `script` node:

```
<project default="all" basedir=".">
  <taskdef name ="txst" classname="oracle.tuxedo.jmx.tux.jyscript.TXSTTask" />
  <target name="getParameters">
    <txst debug="false" failOnError="false" executeScriptBeforeFile="true"
fileName="./test.py">
      <script>
        connect("//slce04cn03:5067","simpapp","38175")
        cmo.GetParameters()
      </script>
    </txst>
  </target>
</project>
```

TXST does not support Maven in this version.

2.1.3.5 Exiting TXST

To exit TXST:

```
txst:simpapp_38075:/>exit()

c:\jython\bin>
```

2.1.3.6 Getting Help

To display information about TXST commands, print the command's documentation string.

For example, to display information about the disconnect command, enter the following command:

```
txst:/simpapp>help('disconnect')
```

The command returns the following:

```
This function is used to disconnect from tuxedo server instance.

Arguments list:

()

txst: /simpapp > disconnect()
```

2.1.3.7 Recording User Interactions

To start and stop the recording of all TXST command input, enter:

```
startRecording(outputFile)

stopRecording()
```

You must specify the file pathname for storing TXST commands when you enter the startRecording command.

For example, to record TXST commands in the record.py file, enter the following command:

```
txst:/simpapp> startRecording('record.py')
```

For more information, see startRecording and stopRecording.

2.1.3.8 Redirecting TXST Output to a File

To start and stop redirecting TXST output to a file, enter:

```
redirect(outputFile,[toStdOut])

stopRedirect()
```

You must specify the pathname of the file to which you want to redirect TXST output. You can also optionally specify whether you want TXST output to be sent to stdout; the toStdOut argument defaults to True.

For example, to redirect TXST output to the logs/txst.log file in the current directory and disable output from being sent to stdout, enter the following command:

```
txst:/simpapp> redirect('./logs/txst.log',False)
```

For more information, see redirect and stopRedirect.

2.2 Navigating MBeans

- Navigating and Interrogating Mbeans
- Browsing Runtime MBeans
- Finding MBeans

2.2.1 Navigating and Interrogating Mbeans

TXST online provides simplified access to MBeans. While JMX APIs require you to use JMX object names to interrogate MBeans, TXST enables you to navigate a hierarchy of MBeans in a similar fashion to navigating a hierarchy of files in a file system.

Tuxedo organizes its MBeans in a hierarchical data model. In the TXST file system, MBean hierarchies correspond to drives; MBean instances are directories; MBean attributes and operations are files. TXST traverses the hierarchical structure of MBeans using commands such as cd, ls, and pwd in a similar way that you would navigate a file system in a UNIX or Windows command shell. After navigating to an MBean instance, you interact with the MBean using TXST commands.

In the hierarchy, the root directory is DomainMBean; each instance of the MBean type is a subdirectory; and MBean attributes and parameters are nodes (like files) under the MBean instance directory.

```
Domain MBean
  Machine MBean
    Bridge MBean
      Group MBean
        Server MBean
  ARTBatchSystem Mbean
```

- Changing the Current Management Object
- Navigating and Displaying Configuration MBeans Example

2.2.1.1 Changing the Current Management Object

When TXST first connects to an instance of Tuxedo domain, the variable, cmo (Current Management Object), is initialized to the root of all configuration management objects, DomainMBean. When you navigate to an MBean type, the value of cmo reflects the parent MBean. When you navigate to an MBean instance, TXST changes the value of cmo to be the current MBean instance, as shown in the code snippet below:

For more information on TXST variables,see TXST Command and Variable Reference.

Example 2-1 Changing the Current Management Object

```
txst:/offline>connect("//slce04cn03:5035", "simpapp", "58103")
txst:simpapp_58103:/>cmo.getMbeanName()
simpapp_58103:type=tuxedo_domain
txst:simpapp_58103:/>cd('L1')
txst:simpapp_58103:/L1>cmo.getMbeanName()
simpapp_58103:type=tuxedo_machine,LMID=L1
```

2.2.1.2 Navigating and Displaying Configuration MBeans Example

The commands in the example below instruct TXST to connect to a Tuxedo domain instance, navigate, and display MBeans in the DomainMBean. If no argument is specified, then the ls command lists all the child MBeans and attributes

Example 2-2 Navigating and Displaying Configuration MBeans

```
txst:/offline>connect("//slce04cn03:5035", "simpapp", "58103")
txst:simpapp_58103:/>ls()
attributes:
State ACTIVE
parameters:
TA_AUTHSVC
TA_AUTOTRAN N
TA_BBLQUERY 30
TA_BLOCKTIME 6
```

```
TA_CLASS T_DOMAIN
TA_CMTRET COMPLETE
TA_COMPONENTS
TA_CURDRT 0
TA_CURGROUPS 1
TA_CURINTERFACES 0
TA_CURMACHINES 0
TA_CURQUEUES 2
TA_CURRFT 0
TA_CURRTDATA 0
TA_CURSERVERS 2
TA_CURSERVICES 9
TA_CURSTYPE 1
TA_CURTYPE 12
TA_DBBLFAILOVER 0
TA_DBBLWAIT 2
TA_DOMAINID simpapp
TA_ENCRYPTION_REQUIRED N
TA_ERROR 0
TA_GID 8500
TA_HWDRT 0
TA_HWGROUPS 1
TA_HWINTERFACES 0
TA_HWMACHINES 1
TA_HWQUEUES 2
TA_HWRFT 0
TA_HWRTDATA 0
TA_HWSERVERS 2
TA_HWSERVICES 9
TA_INSTANCE_AFFINITY NONE
TA_IPCKEY 58103
TA_LDBAL N
TA_LICEXPIRE
TA_LICMAXUSERS 10000000
TA_LICSERIAL
TA_MASTER L1
TA_MAXACCESSERS 15
TA_MAXACLGROUPS 16384
TA_MAXBUFSTYPE 32
TA_MAXBUFTYPE 16
TA_MAXCONV 1
TA_MAXDRT 0
TA_MAXGROUPS 100
TA_MAXGTT 100
TA_MAXINTERFACES 150
TA_MAXMACHINES 256
TA_MAXNETGROUPS 8
TA_MAXOBJECTS 1000
TA_MAXQUEUES 20
TA_MAXRFT 0
TA_MAXRTDATA 8
TA_MAXSERVERS 20
TA_MAXSERVICES 50
TA_MAXSPDATA 18504
TA_MAXTRANTIME 0
TA_MIBMASK 0
```

```
TA_MODEL SHM
TA_MORE 0
TA_NOTIFY SIGNAL
TA_OCCURS 1
TA_OPTIONS
TA_PERM 384
TA_PREFERENCES
TA_SANITYSCAN 12
TA_SCANUNIT 10
TA_SCANUNIT_EXT 10
TA_SECURITY NONE
TA_SEC_PRINCIPAL_LOCATION
TA_SEC_PRINCIPAL_NAME
TA_SEC_PRINCIPAL_PASSVAR
TA_SGRPFAILOVER 0
TA_SIGNATURE_AHEAD 3600
TA_SIGNATURE_BEHIND 604800
TA_SIGNATURE_REQUIRED N
TA_SSL_RENEGOTIATION 0
TA_STATE ACTIVE
TA_SYSTEM_ACCESS FASTPATH
TA_TRANTIME 30
TA_UID 532
TA_USIGNAL SIGUSR2
childBean:
tuxedo_machine L1
additional info:
```

2.2.2 Browsing Runtime MBeans

Lists all the children beans and/or attributes for the current bean.

You can optionally control the output by specifying an argument. If no argument is specified, the command lists all children beans and attributes in the domain. The output is returned as a string.

2.2.3 Finding MBeans

To locate a particular MBean, you can use the find command. TXST returns the pathname to the specified MBean. You can use the getMBean command to return the MBean specified by the path. For more information, see find and getMBean.

Example 2-3 Finding MBeans

```
txst:simpapp_58103:/>find('ser*')
/L1/GROUP1/server_1
txst:simpapp_58103:/>bean = getMBean('/L1/GROUP1/server_1')
txst:simpapp_58103:/>path = getPath(bean)
txst:simpapp_58103:/>print path
/L1/GROUP1/server_1
```

2.3 Managing the Server Life Cycle

During its lifetime, a running instance can transition through a number of operational states, such as shutdown, starting, suspended, resuming, and running. TXST commands such as start, suspend, resume, and shutdown cause specific changes to the state of a server instance.

Using TXST, you can:

- Start and shutdown a Tuxedo domain, machine, group or server. See Starting and Stopping.
- Migrate the servers in the specified scope to an alternate location.
- Suspend and resume a specified target. See Suspending and Resuming.
- Starting and Stopping
- Suspending and Resuming

2.3.1 Starting and Stopping

TXST provides several ways to start and stop a specified object. The method that you choose depends on the target object.

- Domain
- Machine, Group, and Server

2.3.1.1 Domain

To start a Tuxedo domain, you should invoke startDomain() command. This command must use while TXST is connecting to JMX agent embedded in the tlisten process. If invoking is success, you can connect to Tuxedo domain. See startDomain.

To stop a Tuxedo domain, you should invoke `shutdownDomain()` command. If domain is shutdown successfully, TXST will disconnect from domain and go back to connect JMX agent. See ShutdownDomain.

2.3.1.2 Machine, Group, and Server

For machine, group and server, you can invoke start() or shutdown() directly. If your target is server, there are two ways to operate these command. See Start and Shutdown.

2.3.2 Suspending and Resuming

The following MBeans are supported by suspending and resuming: Machine, Server, Bridge, WSH, JSH. However, the target object is different from the Mbeans. For more details about targets, refer to following table:

Table 2-2 Details about targets

Mbean	Target
Machine	Client
Server	Service

Table 2-2 (Cont.) Details about targets

Mbean	Target
Bridge	Remote bridge
WSH	WSH
JSH	JSH

3
TSAM Plus Accounting and Chargeback

This chapter contains the following sections:

- Accounting Information Output
- Accounting Information Analyzing
- Known Issues

3.1 Accounting Information Output

This section contains the following topics:

- Prerequisite
- Configuration
- Samples

3.1.1 Prerequisite

Before you can use this feature, make sure TSAM Plus agent is installed and TSAM Plus plug-in is enabled.

3.1.2 Configuration

A new option, `-a`, is added to servopts(5) for providing more various accounting information output fields:

```
-a FILENAME[[$FIELD]...]
```

If `-a` option is set, the Tuxedo server prints accounting information into the file specified by `FILENAME`.

The accounting file is generated daily with a file name in the format of `[FILENAME].mmddyy`.

The fields that can be specified for `-a` option are as follows:

- `DID`: Indicates the Tuxedo Domain ID of the server process.
- `LMID`: Indicates the LMID of the server process.
- `GRPID`: Indicates the Tuxedo Group ID of the server process.
- `GRPNAME`: Indicates the Tuxedo Group name of the server process.
- `SID`: Indicates the Tuxedo Server ID of the server process.
- `PID`: Indicates the process ID of the Tuxedo server process.
- `PNAME`: Indicates the process name of the Tuxedo server process.
- `SVC`: Indicates the name of the service being invoked. It always appears in the output fields when `-a` is specified.
- `GID`: Indicates the Tuxedo user group invoking the service.

- `UID`: Indicates the Tuxedo user ID invoking the service.
- `CLIENT`: Indicates the Tuxedo client invoking the service.
- `STIME`: Indicates the time entering the service routing. The output of this field is in the format of `tv_sec/tv_usec`, where two values are expressed as seconds and microseconds since 00:00 Coordinated Universal Time (UTC), January 1, 1970 respectively. It always appears in the output fields when `-a`is specified.
- `ETIME`: Indicates the time leaving the service routing. The output of this field is in the format of “tv_sec/tv_usec”, where two values are expressed as seconds and microseconds since 00:00 Coordinated Universal Time (UTC), January 1, 1970 respectively. It always appears in the output fields when “-a” is specified.
- `TIME`: Indicates the total CPU time (in microsecond) consumed by the service call.
- `SYSTIME`: Indicates the System CPU time (in microsecond) consumed by the service call.
- `USRTIME`: Indicates the User CPU time (in microsecond) consumed by the service call.
- `ERRNO`: Indicates the ERRNO returned to the service invoker.
- `URCODE`: Indicates the URCODE returned to the service invoker.
- `SIZE`: Indicates the size of the request message (in byte).
- `WTIME`: Indicates the waiting time of the request message in a queue (in microsecond).
- `ALL`: Indicates all fields above.
  If no filed is specified for `-a` option, these fields are included in sequence by default: `UID`, `SVC`,`STIME`, `ETIME`, `SYSTIME`, `USRTIME`.

  If a duplicate field name is specified, it is ignored and a warning message is printed in `ULOG: ERROR: duplicate field xxx for -a option`.

  If an invalid field is specified, it is ignored and an error message is printed in `ULOG ERROR: xxx is not a valid field for -a option`.

  The fields separated by TAB character are listed in the first line of a new accounting file. Following is a sample:

  ```
  #UID SVC STIME ETIME SYSTIME USRTIME
  ```

  Subsequently a line is printed for every service call in the same sequence of the field names and values are separated by a TAB character as well. If a field value is not available, it will be left empty.

> **Note**
>
> – A Log file cannot be re-created if it has been deleted when Tuxedo is running.
>
> – If multiple server instances output accounting information to the same file, the same fields in the same sequence must be specified for all relevant servers, otherwise accrpt cannot work.
>
> – The services in system server, such as `BBL, GWTDOMAIN, TMS`, etc. or the system services with the name starting with `'.'` cannot generate accounting records. The following Oracle Tuxedo Application Runtime for CICS servers are supported:
>
> * `ARTATR1`
> * `ARTATRN`
> * `ARTCNX`
> * `ARTDPL`
> * `ARTSTR1`
> * `ARTTDQ`
> * `ARTTSQ`
>
> – A multithread server (built with `-t` option) reports no `TIME`, `SYSTIME` or `USRTIME`.
>
> – A server with the `NONE` or `APP_PW` value of the `SECURITY` parameter in `TUXCONFIG` file reports no `GID`, `UID` or `CLIENT`.

3.1.3 Samples

```
CLOPT="-A -a account_file$SVC$GID$UID$TIME$SIZE --"

CLOPT="-A -a account_file$ALL --"

CLOPT="-A -a account_file --"
```

3.2 Accounting Information Analyzing

You can use a new tool `accrpt` to analyze and aggregate the content of accounting file.

If an accounting file is specified, `accrpt` analyzes and aggregates the file content and print the aggregated information into `STDOUT`.

```
accrpt [-k FIELD[,FIELD]...] [-t {MINUTE|5MINUTES|10MINUTES|15MINUTES|HOUR|DAY}]
[-o FIELD[,FIELD]...] [-i] [FILE(s)]
```

- Configuration
- Output
- Samples

3.2.1 Configuration

-k option

It indicates the key fields separated by ‘,’. The following fields can be specified:

- `DID`: Indicates the Tuxedo Domain ID of the server process.
- `LMID`: Indicates the LMID of the server process.
- `GRPID`: Indicates the Tuxedo Group ID of the server process.
- `GRPNAME`: Indicates the Tuxedo Group name of the server process.
- `SID`: Indicates the Tuxedo Server ID of the server process.
- `PID`: Indicates the process ID of the Tuxedo server process.
- `PNAME`: Indicates the process name of the Tuxedo server process.
- `SVC`: Indicates the name of the service being invoked.
- `GID`: Indicates the Tuxedo user group invoking the service.
- `UID`: Indicates the ID of the Tuxedo user invoking the service.
- `CLIENT`: Indicates the Tuxedo client invoking the service.

If this option is not specified, the `SVC` field is specified by default. If a field is specified but its value is not available, the field will be left empty in the output result.

-t option

It indicates the time window to aggregate the accounting information. If it is not specified, the accounting information is aggregated in hour by default.

-o option

It indicates the measurement fields that are outputted for accounting and chargeback purposes. Fields are separated by ‘,’. The following fields can be specified in the list:

- `TIMES`: Indicates the total invoke times.
- `SUCC`: Indicates the invoke times for returning success.
- `APPFAIL`: Indicates the invoke times for returning application failure.
- `SYSFAIL`: Indicates the invoke times for returning system failure.
- `ELPTIME`: Indicates the total elapse time (in millisecond).
- `TIME`: Indicates the total CPU time (in millisecond).
- `SYSTIME`: Indicates the total System CPU time (in millisecond).
- `USRTIME`: Indicates the total User CPU time (in millisecond).
- `SIZE`: Indicates the total message size (in kilobytes) of the request message.
- `WTIME`: Indicates the average waiting time of the request message in a queue (in microsecond).

By default, fields `TIMES, ELPTIME, SYSTIME`, and `USRTIME` are selected as measurement fields.

-i option

If this option is specified, `accrpt` ignores the line of accounting information where any empty key field is included.

File(s)

Specifies accounting files for analyzing. If no file is specified, `accrpt` reads input from `STDIN`.

3.2.2 Output

`accrpt` analyzes raw accounting information and outputs the aggregated accounting information into `STDOUT`. Three groups of fields are outputted in sequence:

- Implicit fields: include `STIME` and `ETIME` of the time window. They are always printed as the first and second fields.
- Key field: All key fields specified by `–k` option.
- Measurement fields: all fields specified by `–o` option.

`accrpt` prints all fields in one line prefixed #character firstly and all accounting information subsequently, sorted by all Key fields, `STIME`, and `ETIME` in ascending order. In a line, all fields are separated by TAB character. If a value is not available, it is left empty.

3.2.3 Samples

This section contains the following topics:

- Sample 1 - Default Usage
- Sample 2
- Sample 3

3.2.3.1 Sample 1 - Default Usage

For `SimpleServer`, here we set its CLOPT parameter as `-A -a simpserv_acct --` ”

Every day this server outputs its accounting information into a new file named `simpserv_acct.mmddyy`.

```
>cat simpserv_acct.022102
# SVC UID STIME ETIME SYSTIME USRTIME
TOUPPER John 1789249093/34452   1789249093/65389 100 50
......
>accrpt account3. 022102
#STIME ETIME SVC TIMES ELPTIME SYSTIME USRTIME
00:00:00 01:00:00 TOLOWER 10 100 20 40
01:00:00 02:00:00 TOLOWER 15 200 30 50
00:00:00 01:00:00 TOUPPER 10 100 20 40
01:00:00 02:00:00 TOUPPER 10 100 20 40
......
```

3.2.3.2 Sample 2

```
>accrpt –t DAY account.022012
#STIME ETIME SVC TIMES ELPTIME SYSTIME USRTIME
00:00:00 24:00:00 TOLOWER 150 2000 300 500
00:00:00 24:00:00 TOUPPER 100 1000 200 400
```

3.2.3.3 Sample 3

```
>accrpt –k SVC -o TIMES,ELPTIME,TIME,SIZE account1.022012 account3.022012
#STIME ETIME SVC TIMES ELPTIME TIME SIZE
00:00:00 01:00:00 TOLOWER 10 100 20 100
01:00:00 02:00:00 TOLOWER 15 200 30 500
00:00:00 01:00:00 TOUPPER 10 100 20 100
01:00:00 02:00:00 TOUPPER 15 200 30 500
......
```

3.3 Known Issues

- The user ID of an ART service `connect` call is the domain ID. This works by design.
- The ART service `disconnect` cannot be accounted.

4

User Payload Collection

This chapter contains the following topics:

- Overview
- Supported User Payload Buffer Types
- Determine User Payload Storage
- Configuring User Payload Collection
- Exporting Collected User Payload Data

4.1 Overview

Oracle Tuxedo applications send and receive their data in typed buffers. The input message and output message of a Tuxedo service are described in Tuxedo buffer types. TSAM Plus can collect the user payload encapsulated in the Tuxedo service input and output buffer, store the collected payload in Oracle Database, Hadoop or local file, and provide a series of APIs and tools to export the payload for further aggregation and analysis.

4.2 Supported User Payload Buffer Types

The following table lists the supported Oracle Tuxedo buffer types for user payload.

Table 4-1 Supported Oracle Tuxedo Buffer Types in User Payload

Type Name	Description
CARRAY	Character array (possibly containing NULL characters) that is neither encoded nor decoded during transmission
X_OCTET	Equivalent to CARRAY; provided for XATMI compatibility
STRING	NULL-terminated character array
FML	FML fielded buffer
VIEW	C structure or FML view
X_C_TYPE	Equivalent to VIEW; provided for XATMI compatibility
X_COMMON	Equivalent to VIEW; provided for XATMI compatibility
FML32	FML32 fielded buffer, using 32-bit identifiers and offsets
VIEW32	C structure or FML32 view, using 32-bit identifiers, counter variables, and size variables
XML	Buffer for XML documents

4.3 Determine User Payload Storage

TSAM Plus supports different kinds of storage for the collected user payload, which include Oracle Database, Hadoop, and local file.

- User Payload Record in Oracle Database

- User Payload Record in Hadoop
- User Payload Record in Local File
- Specifying User Payload Storage from TSAM Plus Console

4.3.1 User Payload Record in Oracle Database

User payload data is stored in the table MON_PAYLOAD in TSAM plus Database, as listed in the table below.

Table 4-2 User Payload Data in MON_PAYLOAD

COLUMN	TYPE	Nullable	Constraints	Since Version	Description
ID	NUMBER	NO		12.2.2	auto-generated ID
DOMAINID	VARCHAR2(30)	YES		12.2.2	Domain ID, it is null when no DOMAINID is set in UBBCONFIG
LMID	VARCHAR2(30)	YES		12.2.2	Machine LMID
GROUPID	SMALLINT	YES		12.2.2	Tuxedo group number
SERVERID	SMALLINT	YES		12.2.2	Server ID
SVCNAME	VARCHAR2(127)	YES		12.2.2	Service name
CORRELATIONID	VARCHAR2(255)	YES		12.2.2	Call path CORRELATIONID
ECID	VARCHAR2(1024)	YES		12.2.2	Tuxedo call ECID
TPERRNO	SMALLINT	YES		12.2.2	tperrno
VALUETYPEINDEX	SMALLINT	YES		12.2.2	Tuxedo buffer type index, defined in weblogic.wtc.jatmi.StandardTypes CARRAY : 16 STRING : 17 FML : 18 VIEW : 19 X_OCTET : 20 X_C_TYPE : 21 X_COMMON : 22 FML32 : 23 VIEW32 : 24 XML : 25
VALUESUBTYPE	VARCHAR2(127)	YES		12.2.2	Tuxedo sub buffer type. It is the view or view32 name
PAYLOADTYPE	SMALLINT	YES		12.2.2	1 means request; 2 means reply
VALUE	BLOB	YES		12.2.2	User payload value
LOGTIME	TIMESTAMP	YES		12.2.2	The timestamp when this record is reported from TSAM Plus Agent.

4.3.2 User Payload Record in Hadoop

User payload data can be stored in HDFS. It requires JRE 1.7 or above.

To store the payload into the Hadoop file system, you must set the environments `JAVA_HOME` and library path before starting LMS. Additionally, the LMS `-T` option must not be set or set to 1.

For Linux systems, the library path `LD_LIBRARY_PATH` must include the `libjvm.so`

Following is an example for Linux:

```
export JAVA_HOME=/home/user1/jdk1.7.0_21

export HADOOP_HOME=/home/user1/hadoop-2.6.0

export LD_LIBRARY_PATH=$JAVA_HOME/jre/lib/amd64/server/:$LD_LIBRARY_PATH
```

For AIX systems, set `LIBPATH` instead of `LD_LIBRARY_PATH`.

For example:

```
export LIBPATH=/usr/$JAVA_HOME/jre/lib/ppc64/classic:$JAVA_HOME/jre/
libppc64:$JAVA_HOME/jre/lib/ppc64/j9vm
```

- File Naming
- Content Format

4.3.2.1 File Naming

If you choose to output the payload data to Hadoop file system, TSAM Plus generates a payload file to store the payload key and data. Each machine writes a distinct file every day.

The format is `<domain>_<machine>_<yyyymmdd>.payload`. The new hadoop file is produced every day and there is no file size limit.

4.3.2.2 Content Format

TSAM Plus uses the Hadoop SequenceFile format (Hadoop 2.6 ver=6) to store the payload in HDFS. Each payload record includes the key and value data. The record (`org.apache.hadoop.io.BytesWritable`) can be parsed using the Java class `com.oracle.tsam.payload.PayloadRecord`.

The record key class is `org.apache.hadoop.io.LongWritable` and the value class is `org.apache.hadoop.io.BytesWritable`. Both are stored as the record.

Following is the payload SequenceFile format:

- Header
  - version - 3 bytes of the magic header SEQ, followed by 1 byte of actual version number (e.g. SEQ4 or SEQ6)
  - keyClassName - Key class
  - valueClassName - Value class
  - compression - A boolean that specifies if compression is turned on for keys/values in this file. 0 is used for payload file.
  - blockCompression - A boolean that specifies if block compression is turned on for keys/values in this file. 0 is used for payload file.
  - metadata - `SequenceFile.Metadata` for this file. `0x0,0x0,0x0,0x0`
  - sync - A sync marker that denotes the end of the header.

- Record
  - Record length
  - Key length
  - Key
  - Value length
  - Value - Payload record that includes the payload key and value
- A sync-marker.

4.3.3 User Payload Record in Local File

The naming and content format of the user payload record in local file are same as rules on Hadoop.

You can specify the local file directory where the payload data will be stored using the LMS server CLOPT parameter in `UBBCONFIG`. For example, to store the payload data in the file at `/u01/common/patches/oracle/payload`, configure the following in the `UBBCONFIG` file:

```
LMS SRVGRP=LMSGRP SRVID=2 CLOPT="-A -- -l <tsam_manager_host>:7001/tsam -p /u01/
common/patches/oracle/payload"
```

For more information, refer to Local Monitor Server in Oracle TSAM Plus Server, Command, and API Reference Guide.

4.3.4 Specifying User Payload Storage from TSAM Plus Console

To specify the storage method for the user payload data, do the following:

1. From the TSAM Plus console top menu bar, click **Management -> Global Parameters**
2. In the TSAM Plus Global Properties tab, select one of the storage: Database, Hadoop, or local file.
3. If Hadoop is selected, continue specifying the following fields:
   - Hadoop URL:
     Specify the Hadoop URL where you want to store the user payload data. The Hadoop URL must include the hostname, port, and payload file directory. For example: `hdfs://localhost:8080/tmp/tuxPayload/`
4. Click **Modify**.

4.4 Configuring User Payload Collection

You can define user payload data collection policies for services or call path. Take call path for example, to configure collection policies, follow the steps below:

1. From the TSAM Plus console top menu bar, click **Policy-> Tuxedo Monitoring Policy**.
2. In the Monitoring Policy List page, click **Add** to enter the **Edit Policy** page.
3. In the left Tuxedo Component filter area, select the Tuxedo domain to monitor.
4. In the Call path tab, select **Enable** to enable the call path metrics collection.
5. Click the **Define Payload Collection** button to configure payload collection rules.

6. In the Define Payload Collection page, you can enable request and/or response payload collection by selecting the corresponding checkbox. If request payload collection is enabled, you can decide if only collecting the payload for initial called service by selecting **Initial Called Service Only** or not.
7. Click **OK**. Then enable the policy.

> **Note**
>
> The call path user payload data collection policies cannot be propagated to other domains.

Now you have completed the definition of a most general user payload collection policy. All the payload belonging to the defined scope will be collected and saved to the designated payload storage.

You can also narrow down the payload data collection scope by defining collection data criteria or result filter. For more information, see Defining Payload Collection Data Criteria and Defining Payload Collection Result Filter .

- Defining Payload Collection Data Criteria
- Defining Payload Collection Result Filter

4.4.1 Defining Payload Collection Data Criteria

When a data criteria is defined, TSAM Plus collects the payload only if the typed buffer value fulfills the criteria. For example, when a STRING typed buffer starts with the word Hello, or a FML32 typed buffer whose ACCOUNT_ID field has a value larger than 1000, the system collects the payload.

To define the data criteria, do the following steps:

1. Go to the **Data Criteria** tab in the Define Payload Collection dialog. All the supported buffer types are listed in the drop down list.
2. Select the buffer type you want to define a criteria against and then click **Add**.
   A table with the title Add one or multiple data criteria entries is displayed.

Table 4-3 Data Criteria Table

Column Name	Visible for Buffer Type	Description
Field Name	FML/FM32VIEW/ VIEW32X_COMMON/ X_C_TYPE	A single selection drop down list. For FML/FML32, it is the field name in the FML field table definition file. The supported field types are: short, long, float, double, char, and string. Fields with other types are hidden from the drop down list. For all VIEW liked buffer types, it is the VIEW name defined after the VIEW keyword in the VIEW table definition file.
Sub Field Name	VIEW/VIEW32X_COMMON/ X_C_TYPE	A single selection drop down list. The value is the VIEW field name (CNAME) in the VIEW table definition file. The supported field types are same with the FML fields.
Occurrence	FML/FML32	The specific occurrence of a FML field.
Operator	All buffer types	A single selection drop down list. For numeric fields, the options are: >, >=, <, <=, ==, !=For alphabetic fields, the options are: ==, !=, %%, !%

Table 4-3 (Cont.) Data Criteria Table

Column Name	Visible for Buffer Type	Description
Value	All buffer types except XML	A text input box. It is the value part (after the operator) of a FML Boolean Expression. No operators are allowed here.It must fit all the syntax defined by the FML Boolean Expression. For more information about FML Boolean Expression, refer to the online Oracle Tuxedo Documentation. Examples of the value are: • 'Hello.*' (Note the single quote) • 'Hello.*' (Note the single quote) • 1000
Expression	XML	A text input box. A valid XPath expression is expected here.
Direction	All buffer types	This area is made up of three mutually exclusive radio buttons. If both request and response payload collection are enabled in the General tab, all the three radio buttons - Inout, In, and Out are enabled. Otherwise only the corresponding radio button is enabled. If Inout is selected, current criteria expression takes effect for both request and response buffers. If In or Out is selected, only request or response buffer is evaluated against current criteria.
Actions	All buffer types	This column contains one add button and one remove button. Multiple data criteria expression entries can be added to the table. On saving of the policy, each entry forms a FML Boolean expression and different entries in the same table are of the logical AND relationship.

3. Once all the criteria expression entries are defined, click **Submit** to save your configurations.
   After returning to the data criteria listing page, you can find the new-created data criteria in the listing table.

> **Note**
>
> - You can add multiple data criteria for the same buffer type. They are of logical OR relationship. It means that any of the data criteria is satisfied when the payload is collected.
> - For the buffer type `FML32/FML/VIEW32/VIEW/X_C_TYPE/X_COMMON`, the field table definition files must be uploaded in the **Data Management -> Field Tables Management** tab page before defining the data criteria.

4.4.2 Defining Payload Collection Result Filter

The result filter defines for each buffer type, for example, which fields or the char sequence ranges are collected, regardless of the runtime payload data value. Compared to data criteria, it is a relative static definition to filter unnecessary fields out.

Defining the result filter are very similar to the operations of defining data criteria. The differences are:

In the result filter listing page, each buffer type can only be defined with one result filter.

In the result filter entries definition page, different filter entries are of logical OR relationship. This means in the runtime, TSAM Plus tries to collect all the defined entries of a result filter.

> **Note**
>
> If both the result filters for call path and services are enabled on a Tuxedo service call, the filters on the call path take effect.

4.5 Exporting Collected User Payload Data

The user payload data stored in Oracle TSAM Plus database, local file, or Hadoop is in binary format. For ease of data analysis, you can export the data to text format or XML format using the export APIs or payload dump tool.

- APIs for Data Export
- Payload Dump Tool

4.5.1 APIs for Data Export

The following table lists the APIs for exporting the user payload data.

Table 4-4 APIs for Data Export

Category	API	Description
Interface	PayloadRepository	Payload metrics storage interface
Class	FilePayloadIterator	Payload record iterator of file storage
	FilePayloadRepository	File storage of payload metrics
	HadoopPayloadIterator	Payload record iterator of Hadoop storage
	HadoopPayloadRepository	Hadoop storage of payload metrics
	payloaddump	A command line tool dumping payload metrics
	PayloadRecord	Payload record in the storage
	PayloadValue	Payload metrics.
	TSAMDBPayloadIterator	Payload record iterator of TSAM Plus database storage
	TSAMDBPayloadRepository	TSAM Plus database storage of payload metrics
Enum	Enum PayloadType	Payload metrics type

When using API for data export, you must include the following jar in `CLASSPATH` under `$TSAMDIR/lib`:

```
CLASSPATH=payloadapi.jar:com.bea.core.jatmi_2.0.0.0.jar:com.oracle.tuxedo.tjatmi_12.1.3.0.jar:commons-cli-1.2.jar
```

If you want to export the payload from Hadoop dfs, set the `HADOOP_HOME`:

```
HADOOP_HOME=/home/user/hadoop-2.6.0/
```

If you want to export the payload from Oracle Database, include `ojdbc6.jar` in `CLASSPATH`.

- PayloadRepository
- FilePayloadIterator
- FilePayloadRepository
- HadoopPayloadIterator
- HadoopPayloadRepository
- payloaddump
- PayloadRecord
- PayloadValue
- TSAMDBPayloadIterator
- TSAMDBPayloadRepository
- Enum PayloadType
- Payload API Samples

4.5.1.1 PayloadRepository

All Superinterfaces `java.lang.AutoCloseable, java.io.Closeable, java.lang.Iterable<PayloadRecord>`

All Known Implementing Classes `FilePayloadRepository, HadoopPayloadRepository,TSAMDBPayloadRepository`

Description `public interface PayloadRepository extends java.lang.Iterable<PayloadRecord>,java.io.Closeable`

Payload metrics storage interface

4.5.1.2 FilePayloadIterator

`java.lang.Object`

`com.oracle.tsam.payload.FilePayloadIterator`

All Implemented Interfaces

`java.util.Iterator<PayloadRecord>`

Description

`public class FilePayloadIterator extends java.lang.Object implements java.util.Iterator<PayloadRecord>`

Payload record iterator of file storage.

Methods inherited from class java.lang.Object

`equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait`

Constructor Detail

FilePayloadIterator

`public FilePayloadIterator(org.apache.hadoop.io.SequenceFile.Reader reader)`

Constructs a FilePayloadIterator with a reader

Method Detail

hasNext

```
public boolean hasNext()
```

Specified by:

```
hasNext in interface java.util.Iterator<PayloadRecord>
```

next

```
public PayloadRecord next()
```

```
Specified by:
```

```
next in interface java.util.Iterator<PayloadRecord>
```

remove

```
public void remove()
```

```
Specified by:
```

```
remove in interface
```

```
java.util.Iterator<PayloadRecord>
```

4.5.1.3 FilePayloadRepository

FilePayloadRepository

```
java.lang.Object
```

```
com.oracle.tsam.payload.FilePayloadRepository
```

All Implemented Interfaces

```
PayloadRepository, java.io.Closeable,
```

```
java.lang.AutoCloseable, java.lang.Iterable<PayloadRecord>
```

Description

```
public class FilePayloadRepository
```

```
extends java.lang.Object
```

```
implements PayloadRepository
```

File storage of payload metrics.

Methods inherited from class java.lang.Object

```
equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait
```

Constructor Detail

FilePayloadRepository

```
public FilePayloadRepository(java.lang.String path)
```

```
throws java.io.IOException
```

Constructs a FilePayloadRepository with a path

Throws:

`java.io.IOException`

Method Detail

iterator

`public java.util.Iterator<PayloadRecord> iterator()`

Specified by:

`iterator in interface java.lang.Iterable<PayloadRecord>`

close

`public void close()`

`throws java.io.IOException`

Specified by:

`close in interface java.io.Closeable`

Specified by:

`close in interface java.lang.AutoCloseable`

Throws:

java.io.IOException

getFile

`public java.io.File getFile()`

Returns the File object

4.5.1.4 HadoopPayloadIterator

HadoopPayloadIterator

`java.lang.Object`

`com.oracle.tsam.payload.HadoopPayloadIterator`

All Implemented Interfaces

`java.util.Iterator<PayloadRecord>`

Description

`public class HadoopPayloadIterator`

`extends java.lang.Object`

`implements java.util.Iterator<PayloadRecord>`

Payload record iterator of Hadoop storage.

Methods inherited from class java.lang.Object

`equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait`

Constructor Detail

HadoopPayloadIterator

```
public HadoopPayloadIterator(java.lang.String HadoopURL,
java.lang.String[] MatchFiles)
throws java.io.IOException
```

Throws:

```
java.io.IOException
```

Method Detail

hasNext

```
public boolean hasNext()
```

next

```
public PayloadRecord next()
```

Specified by:

next in interface java.util.Iterator<PayloadRecord>

close

```
public void close()
throws java.io.IOException
```

Throws:

java.io.IOException

remove

```
public void remove()
```

Specified by:

remove in interface java.util.Iterator<PayloadRecord>

4.5.1.5 HadoopPayloadRepository

HadoopPayloadRepository

```
java.lang.Object
com.oracle.tsam.payload.HadoopPayloadRepository
```

All Implemented Interfaces

```
PayloadRepository, java.io.Closeable, java.lang.AutoCloseable,
java.lang.Iterable<PayloadRecord>
```

Description

```
public class HadoopPayloadRepository
extends java.lang.Object
```

```
implements PayloadRepository
```

Hadoop storage of payload metrics.

Methods inherited from class java.lang.Object

```
equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait
```

HadoopPayloadRepository

HadoopPayloadIterator

```
public HadoopPayloadRepository(java.lang.String HadoopURL,
java.lang.String Domain,
java.lang.String Machine,
java.util.Date StartDate,
java.util.Date EndDate)
throws java.io.IOException
```

Constructs a HadoopPayloadRepository with a Hadoop URL and filters of domain name, machine name, start date, and end date

Throws:

```
java.io.IOException
```

Method Detail

iterator

```
public java.util.Iterator<PayloadRecord> iterator()
```

Specified by:

```
iterator in interface java.lang.Iterable<PayloadRecord>
```

close

```
public void close()
```

```
throws java.io.IOException
```

Specified by:

close in interface java.io.Closeable

Specified by:

```
close in interface java.lang.AutoCloseable
```

Throws:

java.io.IOException

payloaddump

```
java.lang.Object
```

```
com.oracle.tsam.payload.payloaddump
```

Description

```
public class payloaddump
```

extends java.lang.Object

Constructor Detail

4.5.1.6 payloaddump

java.lang.Object

com.oracle.tsam.payload.payloaddump

Description

public class payloaddump

extends java.lang.Object

A command line tool dumping payload metrics.

Methods inherited from class java.lang.Object

equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait

Constructor Detail

payloaddump

public payloaddump()

Method Detail

main

public static void main(java.lang.String[] args)

throws org.apache.commons.cli.ParseException,

java.lang.ClassNotFoundException,

java.sql.SQLException,

java.io.IOException,

javax.xml.parsers.ParserConfigurationException,

java.text.ParseException,

java.lang.Exception

Parameters:

args

-url

Mandatory parameter. Payload repository URL. It can be a database URL, Hadoop URL, or a file path

-username

Database user name

-password

Database password

-payloadtype

Mandatory parameter. Request or reply

-wherecondition

SQL query condition. It is available only when the URL is specified to a Database URL.

-domainid

The domain ID used to filter the results

-servicename

The service name used to filter the results

-outputtype

XML or text. The default output type is xml.

-fieldnames

Expected field names when the output type is text. For the Tuxedo type CARRAY, X_OCTET, and STRING, the fieldnames is the aliasNames specified in the result filter of the user payload policy. If url is specified to a Database URL and servicename is specified, the default fieldnames is from the service contract information. If url is specified to a Database URL and policyname and servicename are both specified, the default fieldnames is the join result of the service contract information and the result filter of the policy.

-O

Output file name. The default output is standard output.

Throws:

`org.apache.commons.cli.ParseException`

`java.lang.ClassNotFoundExceptionjava.sql.SQLException`

`java.io.IOException`

`javax.xml.parsers.ParserConfigurationException`

`java.text.ParseException`

`java.lang.Exception`

4.5.1.7 PayloadRecord

`java.lang.Object`

`com.oracle.tsam.payload.PayloadRecord`

Description

`public class PayloadRecord`

`extends java.lang.Object`

Payload record in the storage.

Methods inherited from class java.lang.Object

`equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait`

Constructor Detail

PayloadRecord

```
public PayloadRecord(java.lang.String dOMAINID,
java.lang.String LMID,
short groupID,
short serverID,
java.lang.String serviceName,
java.lang.String correlationID,
java.lang.String ECID,
java.lang.Short errno,
PayloadType payloadType,
java.util.Date logtime,
PayloadValue payloadValue)
```

Method Detail

getdOMAINID

```
public java.lang.String getdOMAINID()
```

setdOMAINID

```
public void setdOMAINID(java.lang.String dOMAINID)
```

getLMID

```
public java.lang.String getLMID()
```

setLMID

```
public void setLMID(java.lang.String lMID)
```

getGroupID

```
public short getGroupID()
```

setGroupID

```
public void setGroupID(short groupID)
```

getServerID

```
public short getServerID()
```

setServerID

```
public void setServerID(short serverID)
```

getServiceName

```
public java.lang.String getServiceName()
```

setServiceName

```
public void setServiceName(java.lang.String serviceName)
```

getCorrelationID

```
public java.lang.String getCorrelationID()
```

setCorrelationID

```
public void setCorrelationID(java.lang.String correlationID)
```

getECID

```
public java.lang.String getECID()
```

setECID

```
public void setECID(java.lang.String eCID)
```

getTperrno

```
public PayloadType getPayloadType()
```

setTperrno

```
public void setTperrno(java.lang.Short tperrno)
```

getPayloadType

```
public PayloadType getPayloadType()
```

setPayloadType

```
public void setPayloadType(PayloadType payloadType)
```

getPayloadValue

```
public PayloadValue getPayloadValue()
```

setPayloadValue

```
public void setPayloadValue(PayloadValue payloadValue)
```

getLogtime

```
public java.util.Date getLogtime()
```

setLogtime

```
public void setLogtime(java.util.Date logtime)
```

4.5.1.8 PayloadValue

```
java.lang.Object
```

```
com.oracle.tsam.payload.PayloadValue
```

Description

```
public class PayloadValue
```

```
extends java.lang.Object
```

Payload metrics. It has two kinds of output formats:

- Text: It is same to the Database export format in "text" mode so that it can be imported into a Database table as the BI data source.

  > **Note**
  >
  > You can define the sequence of the output data using String [] fieldNames. If no fieldnames are provided, the fields are outputted in the default order. None of the embedded buffer is outputted.

- XML: The formatter can convert the typed buffer CARRAY, X_OCTET, STRING, FML, FML32, VIEW, VIEW32, X_C_TYPE, X_COMMON, and XML to XML format. If the buffers are nested, all the nested buffers are also converted.
  For CARRAY/X_OCTET/STRING, the payload is converted to an element in XML format. CARRAY is encoded to a base64 string. The element name is the value specified to the parameter elemName.

  For FML/FML32/VIEW/VIEW32/X_C_TYPE/X_COMMON, the formatter converts all the fields in the typed buffer. If these kinds of typed buffers are nested, all the nested buffers are also converted.
  For XML, the formatter makes no change.

  Methods inherited from class java.lang.Object

  `equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait`

  Constructor Detail

  PayloadValue

  ```
  public PayloadValue(short valueTypeIndex,
  byte[] payloadValue)
  ```

Method Detail

getFieldNames

```
public java.lang.String[] getFieldNames()
```

Returns:

The field names in this object

toXMLString

```
public java.lang.String toXMLString(java.lang.String encoding)
throws java.io.IOException, javax.xml.parsers.ParserConfigurationException,
org.xml.sax.SAXException
```

convert payload value to a XML string. **Parameters:**

`encoding`

Parameters:

encoding

Throws:

`java.io.IOException`

`javax.xml.parsers.ParserConfigurationException`

`org.xml.sax.SAXException`

toText

```
public java.lang.String toText(char delimiter,

char enclosure)

throws java.io.IOException,

javax.xml.parsers.ParserConfigurationException,

org.xml.sax.SAXException
```

convert payload value to text, which can be imported into a Database table. The embedded fields are not in the returned value. Characters equaling to the enclosure are duplicated

Parameters:

`delimiter - delimiter character`

```
enclosure - enclosure character
```

Returns:

text

Throws:

```
java.io.IOException

javax.xml.parsers.ParserConfigurationException

org.xml.sax.SAXException
```

toText

```
public java.lang.String toText()

throws java.io.IOException,

javax.xml.parsers.ParserConfigurationException,

org.xml.sax.SAXException
```

convert payload value to text, which can be imported into a Database table, which the default setting of delimiter=tab and enclosure="". the embedded fields are not in the returned value.

Parameters:

```
delimiter -

enclosure -

fieldNames -
```

Returns:

text

Throws:

```
java.io.IOException

javax.xml.parsers.ParserConfigurationException
```

4.5.1.9 TSAMDBPayloadIterator

```
java.lang.Object
com.oracle.tsam.payload.TSAMDBPayloadIterator
```

All Implemented Interfaces

```
java.util.Iterator<PayloadRecord>
```

Description

```
public class TSAMDBPayloadIterator
extends java.lang.Object
implements java.util.Iterator<PayloadRecord>
```

Payload record iterator of TSAM Plus database storage.

Methods inherited from class java.lang.Object

```
equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait
```

Constructor Detail

TSAMDBPayloadIterator

```
public TSAMDBPayloadIterator(java.lang.String whereConditionalExpression,
java.sql.Connection con)
throws java.sql.SQLException
```

Throws:

```
java.sql.SQLException
```

Method Detail

hasNext

```
public boolean hasNext()
```

Specified by:

```
hasNext in interface java.util.Iterator<PayloadRecord>
```

next

```
public PayloadRecord next()
```

Specified by:

```
next in interface java.util.Iterator<PayloadRecord>
```

remove

```
public void remove()
```

Specified by:

```
remove in interface java.util.Iterator<PayloadRecord>
```

4.5.1.10 TSAMDBPayloadRepository

```
java.lang.Object
```

```
com.oracle.tsam.payload.TSAMDBPayloadRepository
```

All Implemented Interfaces

```
PayloadRepository, java.io.Closeable, java.lang.AutoCloseable,
java.lang.Iterable<PayloadRecord>
```

Description

```
public class TSAMDBPayloadRepository
```

```
extends java.lang.Object
```

```
implements PayloadRepository
```

TSAM Plus database storage of payload metrics.

Methods inherited from class java.lang.Object

```
equals, getClass, hashCode, notify, notifyAll, toString, wait, wait, wait
```

Constructor Detail

TSAMDBPayloadRepository

```
public TSAMDBPayloadRepository(java.lang.String TSAMDBURL)
```

```
throws java.sql.SQLException,
```

```
java.lang.ClassNotFoundException
```

Constructs a TSAMDBPayloadRepository with a TSAM Plus database URL

Throws:

```
java.sql.SQLException
```

```
java.lang.ClassNotFoundException
```

TSAMDBPayloadRepository

```
public TSAMDBPayloadRepository(java.sql.Connection connection)
```

Constructs a TSAMDBPayloadRepository with a TSAM Plus database connection

Method Detail

iterator

```
public java.util.Iterator<PayloadRecord> iterator()
```

Specified by:

```
iterator in interface java.lang.Iterable<PayloadRecord>
```

iterator

```
public java.util.Iterator<PayloadRecord> iterator(java.lang.String
WhereConditionalExpression)
```

```
throws java.sql.SQLException
```

Gets an iterator from the input SQL query condition

Parameters:

```
whereConditionalExpression - SQL query condition, for an example, "where
DOMAINID='DOMAIN1' and LMID='L1' and GROUPID=1 and SERVERID=1 and
SVCNAME='toupper' and PAYLOADTYPE=1"
```

```
for an example, "where DOMAINID='DOMAIN1' and LMID='L1' and GROUPID=1 and
SERVERID=1 and SVCNAME='toupper' and PAYLOADTYPE=1"
```

> **Note**
>
> for the field `PAYLOADTYPE`, 1 means request, 2 means reply

Returns:

An iterator

Throws:

```
java.sql.SQLException
```

close

```
public void close()
```

```
throws java.io.IOException
```

Specified by:

close in interface java.io.Closeable

Specified by:

close in interface java.lang.AutoCloseable

Throws:

java.io.IOException

getConnection

```
public java.sql.Connection getConnection()
```

Returns:

TSAM Plus database connection

getFieldNames

```
public java.lang.String[] getFieldNames(java.lang.String domainID,
java.lang.String serviceName, PayloadType payloadType)
```
throws java.lang.Exception

Parameters:

```
domainID - domain ID
```

```
serviceName - service name
```

```
payloadType - payload type
```

Returns:

Field names

Throws:

`java.lang.Exception`

4.5.1.11 Enum PayloadType

`java.lang.Object`

`java.lang.Enum<PayloadType>`

`com.oracle.tsam.payload.PayloadType`

All Implemented Interfaces

`java.io.Serializable, java.lang.Comparable<PayloadType>`

Description

`public enum PayloadType`

`extends java.lang.Enum<PayloadType>`

Payload metrics type.

Methods inherited from class java.lang.Enum

`compareTo, equals, getDeclaringClass, hashCode, name, ordinal, toString, valueOf`

Methods inherited from class java.lang.Object

`getClass, notify, notifyAll, wait, wait, wait`

Enum Constant Detail

request

`public static final PayloadType request`

Request of a Tuxedo call

Method Detail

values

`public static PayloadType[] values()`

Returns an array containing the constants of this enum type, in the order they are declared. This method may be used to iterate over the constants as follows:

```
for (PayloadType c : PayloadType.values())
System.out.println(c);
```

Returns:

an array containing the constants of this enum type, in the order they are declared

valueOf

`public static PayloadType valueOf(java.lang.String name)`

Returns the enum constant of this type with the specified name. The string must match exactly an identifier used to declare an enum constant in this type. (Extraneous whitespace characters are not permitted.)

Parameters:

name - the name of the enum constant to be returned.

Returns:

The enum constant with the specified name

Throws:

`java.lang.IllegalArgumentException` - if this enum type has no constant with the `specified name java.lang.NullPointerException` - if the argument is null

4.5.1.12 Payload API Samples

The following shows an example that reads payload metrics from TSAM Plus database, and exports the data to a text file.

Example 4-1 API Sample 1

```
public class DBPayloadSample {

  public static void main(String[] args) throws IOException {

    TSAMDBPayloadRepository tSAMDBPayloadRecordRepository = new
TSAMDBPayloadRepository(
      "jdbc:oracle:thin:@localhost:1521:orcl",
      "tsam", "tsam");

    Iterator < PayloadRecord > iterator = tSAMDBPayloadRecordRepository
      .iterator("where DOMAINID='DOMAIN1' and svcname='toupper' and
PAYLOADTYPE=1");

    String[] fieldNames = tSAMDBPayloadRecordRepository.getFieldNames(
      "DOMAIN1", "toupper", PayloadType.request);

    Writer writer = new FileWriter("payload.txt");

    for (int i = 0; i < fieldNames.length - 1; i++) {
      writer.append("\"" + fieldNames[i] + "\"\t");
    }
    writer.append("\"" + fieldNames[fieldNames.length - 1] + "\"");

    while (iterator.hasNext()) {
      {
        PayloadValue payloadValue = iterator.next().getPayloadValue();

        writer.append(payloadValue.toText(fieldNames));
        writer.append('\n');
      }
    }

    writer.close();
```

```
    tSAMDBPayloadRecordRepository.close();

  }
}
```

The output format of the file "payload.txt" is

```
"STRINGFIELD1 ""STRINGFIELD2 ""INTFIELD1 ""SHORTFIELD1"
"abc" "def" "10000" ""
"hij" "" "1" "2"
```

The following is an example that reads payload metrics from Hadoop, and exports the data to an XML file.

Example 4-2 Payload API Sample 2

```
public class HadoopPayloadSample {

  public static void main(String[] args) throws IOException {

    HadoopPayloadRepository hadoopPayloadRecordRepository = new
HadoopPayloadRepository(
      "hdfs://localhost:8080/tmp/tuxPayload/");

    Iterator < PayloadRecord > iterator = hadoopPayloadRecordRepository
      .iterator();

    Writer writer = new FileWriter("payload.txt");

    while (iterator.hasNext()) {
      PayloadRecord payloadRecord = iterator.next();
      if ("DOMAIN1".equals(payloadRecord.getdOMAINID()) &&
        "toupper".equals(payloadRecord.getServiceName()) &&
        (payloadRecord.getPayloadType() == PayloadType.request)) {

        PayloadValue payloadValue = iterator.next().getPayloadValue();

        writer.append(payloadValue.toXml());
        writer.append('\n');

      }
    }

    writer.close();

    hadoopPayloadRecordRepository.close();
  }

}
```

4.5.2 Payload Dump Tool

Before running the payload dump tool, you must configure the following:

- Set the `CLASS PATH` as follows:
  `CLASSPATH=payloadapi.jar:com.bea.core.jatmi_2.0.0.0.jar:com.oracle.tuxedo.tjatmi_12.1.3.0.jar:commons-cli-1.2.jar`
- If you want to export the payload from Hadoop dfs, set the `HADOOP_HOME`:
  `export HADOOP_HOME=/home/user/hadoop-2.6.0/`
- If you want to export the payload from Oracle Database, include `ojdbc6.jar` in `CLASSPATH`.

The payload dump tool command is in the following format:

```
payloaddump -url <URL> [-username <username> -password <password>] -
payloadtype request|reply
[-wherecondition <wherecondition>] [-domainid <domainid>] [-servicename
<servicename>]
[-outputtype xml|text] [-fieldnames <fieldnames>] [-o outputFile]
```

For each parameter description, refer to payloaddump.

For example, to export the payload from Hadoop, run the following command:

```
java com.oracle.tsam.payload.payloaddump -url
"hdfs://localhost:9000/data/" -payloadtype reply -outputtype xml
```

To export the payload from TSAM Plus Database, run the following command:

```
java com.oracle.tsam.payload.payloaddump -url
"jdbc:oracle:thin:@localhost:1521:tsam" -username tsam -password
tsam -payloadtype reply -outputtype xml
```

5

Using Test Load Generator

This chapter contains the following topics:

- Overview
- Creating Call Path Policy for a Replay
- Creating a Replay Definition
- Running a Replay
- Running a Replay in Auto-Created Test Domain

5.1 Overview

Test load generator is a Tuxedo applications load test tool that facilitates effective and efficient load testing. This feature works in conjunction with the payload collection feature to capture the call path and payload metrics coming from a domain gateway, Web service client or application server. One can create replay definition from call paths and execute the replay based on policies for standard and stress test modes.

5.2 Creating Call Path Policy for a Replay

A replay can be constructed from one or more call paths.

In order to collect call path and payload metrics, you need to create a call path policy on the target service with payload collection enabled by doing these steps:

1. From the TSAM Plus console top menu bar, click **Policy-> Tuxedo Monitoring Policy**
2. In the Monitoring Policy List page, click **Add** to enter the **Create Policy** page.
3. In the Call path tab, select to **Enable** to enable the call path metrics.
4. Select the domain in which payload data will be collected in the left **Domain** list, the **Define Payload Collection** button is activated. Click the button.
5. In the Define Payload Collection page, enable request and response payload collection by selecting the corresponding checkbox.
   It is recommended you select **Initial Called Service Only** to avoid collecting unnecessary metrics. The payload collection must not include any result filter.

5.3 Creating a Replay Definition

After the call path policy for the replay is created, do one or more Tuxedo calls to collect the source metrics from call paths. Then you can create a replay definition from call paths by doing these steps:

1. From the TSAM Plus console top menu bar, click **Load Generator-> Replay Definition**.
2. Click **Add**. The Call Path Query and Call Path Result Panels are displayed.
3. Set the query filter options and click **Query**. The desired call paths are displayed in the result panel.

4. Select the call path from the list and click **Create Replay Definition**.
   The new-created replay definition is displayed in the Replay Definition list.

- Setting Replay Definition Attributes

5.3.1 Setting Replay Definition Attributes

You can edit the replay definition attributes.

The following table lists replay definition attributes.

Table 5-1 Replay Definition Attributes

Attribute	Description	Default Value	Editable
name	Replay definition name	-	yes
Tuxedo user name	The Tuxedo user name used to do `tpinit()`	-	yes
Tuxedo client name	The Tuxedo client name used to do `tpinit()`	-	yes
Tuxedo group name	The Tuxedo client name used to do `tpinit()`	-	yes
transaction calls	Call `tpbegin()`when starting the call(s), and call `tpcommit()` when ending the calls	From source call path metrics	yes
transaction parameters	Call `tpbegin()` when starting the call(s), and call `tpcommit()` when ending the calls	From source XA metrics	no
break when any call fails	Whether to break when any call fails. Its value is yes or no.	-	yes
create time	The time when the definition was created	-	no
modify time	The time when the definition was modified	-	no

The default service call attributes are from the first called service (not the "Initial Called Service" in the call path when the initiator is a server) when the replay definition is constructed from call path metrics. The following table lists service calls attributes of replay definition.

Table 5-2 Replay Definition Service Calls Attributes

Attribute	Default Value	Editable
service name	From source metrics	No
source correlation ID	From source metrics	No
call flag "TPNOTRAN"	From the source metrics	Yes
call flag "TPNOCHANGE"	From the source metrics	Yes
call flag "TPNOCOPY"	From the source metrics	Yes
call flag "TPNOBLOCK"	From the source metrics	Yes
call flag "TPNOTIME"	From the source metrics	Yes
call flag "TPSIGRSTRT"	From the source metrics	Yes

5.4 Running a Replay

To run a replay, execute a replay agent in the command line with the exported replay definition file. TSAM Plus replay agents are under `$TUXDIR/bin/`. There are two kinds of agents:

- `tsamreplayagent`
  It supports `tpcall()/tpacall()/tpgetrply()` calls.

- `tsamreplaywagent`
  It supports `tpcall()/tpacall()/tpgetrply()` calls in the workstation mode.

  Before running a replay, make sure the target Tuxedo domain is started up. If TSAM Plus metrics are expected, you must create corresponding policies in TSAM Plus.

> **Note**
>
> The evaluation unit of throughput, latency, success/fail number is the whole replay definition, not one call in it.

The following table lists the replay agent parameters.

Table 5-3 Replay Agent Parameters

Parameter	Description
-p	Invokes the execution plan file when running a replay. Refer to Execution Plan File.
-f	The path of the security profile to be generated. Refer to Replay Security Profile.

- Execution Plan File
- Replay Security Profile
- Replay Execution Result

5.4.1 Execution Plan File

An execution plan file stores a replay execution plan attributes. The attribute format is "`NAME=VALUE`". The attribute name is case-insensitive.

There are two types of execution plan modes, normal mode and stress test mode. The following table lists the general attribute.

Table 5-4 General Attribute

Attribute	Description	Default Value
`definitionFile`	Definition file name	-

- Normal Mode Attributes
- Stress Test Mode Attributes

5.4.1.1 Normal Mode Attributes

The normal mode is the default mode. It is normally used to do unit test or diagnostic a service call. It can also be used to do a stress test by setting the parameters `concurrency number` and `repeat times` to huge values.

Table 5-5 Normal Mode Attributes

Attribute	Description	Default Value
concurrencyNumber	Concurrency number	1

Table 5-5 (Cont.) Normal Mode Attributes

Attribute	Description	Default Value
repeatTime	Repeat time	1
sleepTime	Sleep time when repeating in seconds	0
compareReply	Compares the reply with the one in the replay definition	False

Following is an execution plan file example:

```
definitionFile=def1.xml

concurrencyNumber=10

repeattime=100

sleepTime=0

compareReply=true
```

5.4.1.2 Stress Test Mode Attributes

There are three test mode types:

- Increase the load till the throughput does not increase any longer.
  Following is an execution plan file example:

  ```
  definitionFile=def1.xml

  timeWindow=20

  minCurrency=10

  maxCurrency=1000

  iniCurrency=10

  totalRunTime=3600
  ```

- Increase the load till the max/average latency reaches the specified value. It is enabled when the parameter `maxLatency` or `avgLatency` is specified.

  > **Note**
  >
  > If both `maxLatency` and `avgLatency` are specified, `maxLatency` is ignored.

  Following is an execution plan file example:

  ```
  definitionFile=def1.xml

  timeWindow=20

  minCurrency=10

  maxCurrency=1000

  iniCurrency=10

  maxLatency=1000
  ```

```
avgLatency=500

totalRunTime=3600
```

- Run with the specified throughput. It is enabled when the parameter `throughput` is specified.
  Following is an execution plan file example:

```
definitionFile=def1.xml

timeWindow=20

throughput=1000

totalRunTime=3600
```

Table 5-6 Stress Test Mode Attributes

Attribute	Description	Default Value
`timeWindow`	Load increasing/decreasing time window in seconds	30 seconds
`minCurrency`	Minimum concurrency number limitation. The concurrency number is always not less than it.	1
`maxCurrency`	Maximum concurrency number limitation. The concurrency number is always not greater than it.	10240
`iniCurrency`	The initial concurrency number when the replay starts.	1
`maxLatency`	Maximum latency in microseconds	-
`avgLatency`	Average latency in microseconds	-
`throughput`	Run with the specified throughput per second	-
`totalRunTime`	Total running time in seconds	No limitation

5.4.2 Replay Security Profile

`genreplayprofile` is under `$TUXDIR/bin`. Its parameter is the path of the security profile to be generated. When genreplayprofile is launched, you are prompted to enter the Oracle Tuxedo application password, user name and user password. It generates the replay security profile with the inputted content. The inputted content is used by the replay agent to do tpinit(). If different user names are specified in the replay security profile and the replay definition, the one in the replay security profile takes effect.

5.4.3 Replay Execution Result

Replay execution result is outputted to the standard output after the replay is finished or cancelled.

The normal schedule mode result contains the following contents:

- Submit Time
- End Time
- Success number
- Failure number
- Throughput per second

- Average latency in microseconds
- Identical replies
- Different replies

The stress schedule mode result contains the following contents:

- Detailed information in every 30-second execution time window, including:
  - Current time Success number
  - Failed number
  - Throughput
  - Average latency
  - Concurrency number
- Replay summary
  - Submit Time
  - End Time
  - Success number
  - Failure number
  - Max Throughput per second when the test is ending
  - Minimum latency in microseconds when the test is ending
  - Maximun latency in microseconds when the test is ending
  - Average latency in microseconds when the test is ending
  - Concurrency number when the test is ending

5.5 Running a Replay in Auto-Created Test Domain

You can use the tool `tlgdomgen.py` to create a test domain to call the service in the target domain. The tool is under `$TUXDIR/bin` and can be run using either python or Tuxedo Script Tool (TXST).

- Configuration File
- Executing tlgdomgen.py

5.5.1 Configuration File

Before running *tlgdomgen.py*, you need to create the domain configuration file.

The following table lists the configuration file parameters.

Table 5-7 Configuration File Parameters

Parameter	Description
LDOMPORT	Mandatory. Local access point port of the GWTDOMAIN in the test domain
TUXDIR	Mandatory. TUXDIR of the test domain
APPDIR	Mandatory. APPDIR of the test domain
RDOMID	Mandatory. Access point ID of the GWTDOMAIN in the target domain

Table 5-7 (Cont.) Configuration File Parameters

Parameter	Description
RDOMPORT	Mandatory. Access point port of the GWTDOMAIN in the target domain
RDOMHOST	Mandatory. Access point hostname of the GWTDOMAIN in the target domain
IMPORTSERVICES	List of service names to be imported to the test domain, delimited by space
TSAMMGRHOST	Hostname of the TSAM Plus Manager to be connected by the test domain. LMS is not configured if this item is not specified
LDOMID	Access point ID of the GWTDOMAIN in the test domain
IPCKEY	IPCKEY of the test domain
TSAMMGRPORT	Port of the TSAM Plus Manager to be connected by the test domain. LMS is not configured if this item is not specified

Following is a configuration file example:

```
[Input]
LDOMPORT = 8888
TUXDIR = /home/beadev/bea_linux64.13c/tuxedo12.2.2.0.0
APPDIR = /home/beadev/applicationgrid/domains/domain4
RDOMID = DOMAIN2
RDOMPORT = 6666
RDOMHOST = localhost
```

5.5.2 Executing tlgdomgen.py

To run `tlgdomgen.py` using TXST, do these steps:

1. set Tuxedo environment:
   `$TUXDIR/tux.env`
2. set TXST environment:
   export CLASSPATH=$CLASSPATH:$TUXDIR/jmx/jython-standalone.jar:$TUXDIR/jmx/tmjmx_tux.jar:$TUXDIR/jmx/tmjmx_metadata.jar:$TUXDIR/udataobj/tuxj/com.bea.core.jatmi_2.0.0.0.jar
3. run `tlgdomgen.py`:
   `java oracle.tuxedo.TXST $TUXDIR/bin/tlgdomgen.py <configuration file name>`

   The following files are generated:

   - `ubbconfig.test`: `UBBCONFIG` of the test domain.
   - `addrom.mib`: MIB scripts to add `GWTDOMAIN` access point to the target domain.
   - `setenv.test`: `setenv` of the test domain.
   - `run.sh`: execution scripts to set up and run the test domain.
   - `dmconfig.test`: `DMCONFIG` of the test domain.
4. In the target domain, run the following commands to add the test domain to the target domain:

   ```
   . $TUXDIR/tux.env

   export FLDTBLDIR32=$TUXDIR/udataobj

   export FIELDTBLS32="tpadm,Usysfl32"
   ```

```
ud32 -C tpsysadm < addrom.mib
```

5. Boot the test domain using the file `run.sh`, and then run the replay.

A

Examples of Questions Users Can Ask Through the Operations Assistant

In this release, following are a few examples of questions users can ask through the Operations Assistant. They are grouped by category for easier navigation.

- Product Overview and Release Information
- Getting Started to Use TSAM Plus
- Capacity, Scaling, and Data Management
- Monitoring Configuration and Policies
- Dashboard, Performance, and Health
- Troubleshooting and Logs
- Security
- Alerts
- Domain, Group, Server, and Service Queries
- Call Path, Transaction, Payload, and Runtime Queries

A.1 Product Overview and Release Information

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Product Overview and Release Information category .

- What's Tuxedo?
- What's TSAM Plus?
- Where can we download the new TSAM Plus patch?
- What's the release number and patch level of TSAM Plus? list all the global parameters that users can change?
- What are the known issues/bugs in current version?

A.2 Getting Started to Use TSAM Plus

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Getting Started to Use TSAM Plus category:

- After installing TSAM Plus Manager, how do I get started using it?
- How to use TSAM Plus manager? How to define a call path policy for a domain? How to check the monitored metrics related to the policy just defined. How to define an alert? How to check if there are any alerts related to the alert definition?
- How to reset TSAM Plus admin password?
- How to reset TSAM Plus admin password if I'm unable to login to TSAM Plus console?
- Can a TSAM Plus's User account be Locked/Suspended for a limited period?

- How to change TSAM Plus manager log levels? Which menu should be used to change log levels?
- How to monitor GWWS status? How to monitor GWWS server status? How to monitor GWWS server status such as down, active, etc. via TSAM Plus?

A.3 Capacity, Scaling, and Data Management

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Capacity, Scaling, and Data Management category:

- How many Domains can be monitored safely using a single TSAM Plus?
- Can TSAM Plus Manager be scaled?
- Is there any limit on number of Policies that can be created? Any impact if more are created?
- Can we Archive TSAM Plus's data and restore it back if required?

A.4 Monitoring Configuration and Policies

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Monitoring Configuration and Policies category:

- What's the monitoring policy?
- How to define a TSAM Plus policy to monitor Tuxedo calls?
- What should I do to monitor Tuxedo using TSAM Plus console?
- How to configure a policy to monitor a domain. Explain each item in Domain tree pane?
- How to find out the dependency of a service?

A.5 Dashboard, Performance, and Health

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Dashboard, Performance, and Health category:

- What percentage thresholds define red, yellow, and green status on the Dashboard?
- How to check the performance data, such as throughput, average execution time?
- How to check if a domain is healthy via TSAM Plus console?
- Where to check the health history. How to check the health history of a domain?
- How to monitor the status of a server in a monitored Tuxedo domain? Here the status means up, down, or crashed?

A.6 Troubleshooting and Logs

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Troubleshooting and Logs category:

- If there is any DB connectivity issue in TSAM Plus, which log file to check?
- How to increase LMS agent queue depth as several messages are getting dropped? In what circumstances messages will be dropped by LMS? What are all the possible solutions?

A.7 Security

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Security category:

- How to enable JWT ATN in GWWS?
- How to enable TLS on TSAM Plus agent?

A.8 Alerts

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Alerts category:

- How to check if critical alerts occur?
- How many critical alerts are there in the system?
- Provide all details for the latest fatal alert, including the following fields: name, domain, machine, group, process name, server ID, process ID, time of occurrence, severity, time cleared, alert type, reason, status, and version.
- List all alert definitions and categorize them in Tuxedo, ART CICS, ART Batch and ART IMS, with the detailed information, including name, associated region id, status, severity, type, agent type, expression, mode, alert action, resource filter, filter mode, tuxedo event name if any, interval, time created and modified.
- How many Information alerts in the past 24 hours? List them with details if any.

A.9 Domain, Group, Server, and Service Queries

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Domain, Group, Server, and Service Queries category:

- List the *[groupname]* group with domain name, associated machine id, groupname, its id and status.
- List the LDOM information in the *[domain_name]* domain, and provide the information: local domain access point, local domain id, the associated groupname, its status, Type and tuxedo domain id. In the results, map the ids to their names if the ids are numeric.
- Provide the information about the server *[server name]* with group name, group id, server id, its clopt and machine id. Map the ids to their names and bold the names.
- Which server provides the service *[service name]*, and what's its function name and status, and the related server id? catalog the results under the related domain name. Map the ids to their names and bold the names.
- For the MP domain, provide the following information for each node in the domain: tuxedo domain id, its name, status, tuxedo version.
- List all RDOMs in the *[domain name]* domain, and provide the information as well: remote domain access point, remote domain id, its status, and type. In the results, map the ids to their names if the ids are numeric.
- List all monitored domains and group them in models (SHM or MP domain), with the information: full domain name, master node, and status. How many domains are being monitored?

A.10 Call Path, Transaction, Payload, and Runtime Queries

The following are a few examples of questions users can ask through the Operations Assistant. This section contains Call Path, Transaction, Payload, and Runtime Queries category:

- Provide the last call path information.
- List the last failed call path that has XA transaction enabled.
- List the last user payload data with the maximum possible detail.
- How many calls came from /ws client?
- Any tpcalls with IPC queue length exceeded 3?
- List all the failed tpcalls, or list all the failed calls.