



BEA TSAM™

Tuxedo System and Application Monitor (TSAM) User's Guide

Contents

1. BEA TSAM Console

Overview	1-1
Monitoring Center	1-1

BEA TSAM Console

This section contains the following topics:

- [Overview](#)
- [Monitoring Center](#)

Overview

The BEA TSAM monitoring console defines the Tuxedo components you want to monitor as well as track events and alerts. The TSAM console is composed of two sections:

[Monitoring Center](#): Defines monitoring components and alerts

[Recent Events](#): Tracks event or alert results defined in the monitoring center.

Monitoring Center

[Administration](#)

[Call Path](#)

[Service](#)

[System Server](#)

[Transaction](#)

[Alerts](#)

Administration

[User Management](#)

[Policy Management](#)

[Tuxedo Configuration](#)

[Data Management](#)

User Management

User Management allows you to control and set up who can access and manage the TSAM console. All authorized users are listed on the User Management page. You can add or delete users, as well as change passwords and descriptions.

[Table 1-1](#) lists the User Management page properties.

Table 1-1 User Management Page

Name	Description
User Name	User name
Description	Describes user

Note: A super-user admin is created (by default) without a password. When you log in for the first time, you are requested to enter the super-user admin password.

Add New User

Click the **Add New User** button to add a new user. The **Add New User** page appears.

Note: Only super-user admin can add new users.

[Table 1-2](#) lists the Add New User page properties.

Table 1-2 Add New User Page

Name	Description
User Name	New user name
Password	Enter password[4..15]

Table 1-2 Add New User Page

Name	Description
Confirm Password	Re-enter password[4..15]
Description	Describes user

When you have finished entering the required information, click the **Add User** button to create a new user. If the information is entered correctly, you are returned to the **User Management** page and a new user is added to the user list.

If the information is not entered correctly, you must validate the information and re-enter.

The **Back** button discards new user information and returns you to the **User Management** page.

Change Password

To change a password, do the following steps:

1. Click the check box next to the name of the user whose password you want to change.
2. Click the **Change Password** button.

The **Change User Password** page appears.

Note: Only super-user admin can change user passwords.

[Table 1-3](#) lists the **Change User Password** page properties.

Table 1-3 Change Password Page

Name	Description
User Name	User name[4..15]
Old Password	Enter old password[4..15]
New Password	Enter password[4..15]
Confirm New Password	Re-enter password[4..15]
User Description	Describes user[0..50]

When you have finished entering the required information, click the **Modify** button to change the user password. If the information is entered correctly, you are returned to the **User Management** page.

If the information is not entered correctly, an error message appears.

Change Description

To change a user description, do the following steps:

- 1. Click the check box next to the name of the user whose password you want to change.
- 2. Click the **Change Description** button.

The **Change User Description** page appears.

Note: Only super-user admin can change user descriptions.

[Table 1-3](#) lists the **Change User Description** page properties.

Table 1-4 Change User Description Page

Name	Description
User Name	User name[4..15]
User Description	Enter new user description[0..50]

When you have finished entering the required information, click the **Modify** button to change the user description. If the information is entered correctly, you are returned to the **User Management** page.

If the information is not entered correctly, an error message appears.

Delete User

Click the **Delete User** button at the bottom of **User Management** page is to delete users.

To delete a user, do the following steps:

- 1. Click the check box on the user row to be deleted
- 2. Click the **Delete User** button to delete users.

Notes: Only super-user admin can delete users.

The super-user admin cannot be deleted.

Policy Management

TSAM provides comprehensive monitoring behavior control based on the Tuxedo infrastructure.

Policy Management allows you to do the following:

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

Monitoring Policy Sets Management

The Policy Management page allows you to **Create**, **Edit**, **Clone**, **Import**, and **Delete** monitoring policies. [Table 1-5](#) lists the Monitoring Policy Sets Management page properties.

Table 1-5 Monitoring Policy Sets Management Page

Name	Description
Latest Used Policy Set	TSAM tracks the usage of a defined monitoring policy set. The “latest used” lists the last policy set applied Tuxedo. Editing a policy does not impact this value.
Available Policy Sets	TSAM stores user defined policy sets on the server. All current available policy sets are listed. The directory which holds the policy set definition can be customized using the TSAM Web application file <code>tsam.config.schemesdir</code> in the <code>web.xml</code> .
Name	Name of the policy set.
Last Modified Time	Displays last time the policy set was modified
Create	Creates a new monitoring policy set

Table 1-5 Monitoring Policy Sets Management Page

Name	Description
Edit	Edit an existing monitoring policy set. Only one monitoring policy can be selected at a time.
Clone	Creates a new monitoring policy set by cloning the contents of an existing one. Only one monitoring policy can be selected at a time. The policy set Name and Description attributes will not be copied.
Import	Imports a policy set definition file from desktop and upload to server.
Delete	Deletes one or multiple policy sets

[Table 1-6](#) lists the Monitoring Policy Set File Format properties.

Table 1-6 Monitoring Policy Set File Format

Element Name	Description
TSAM_POLICY	Root tag name of the policy set definition file
NAME	Name of policy set
DESCRIPTION	Policy Set description string
POLICY	A policy in a policy set. You can define multiple policies.
TUXOBJECT	<p>Sub-element of POLICY. It represents which Tuxedo backend policy is impacted by the policy. Its format is:</p> <p>Domain Machine Group Server</p> <p>“Any” is a built-in key word which means any sub-components under the current component. For example, “TUXDOM1 Any APPGRP Any” indicates all servers in the “APPGRP” group of domain “TUXDOM1” are applied to the monitoring policy/</p>
DEFINITION	<p>The monitoring definition string. Has the same format as TMMONITOR.</p> <p>For more information, see Using TSAM Agent in the <i>Tuxedo System and Application Monitor (TSAM) User's Guide</i>.</p> <p>Note: Typically, you will not need to use this element.</p>

Table 1-6 Monitoring Policy Set File Format

Element Name	Description
STATUS	Indicates policy status. 1 indicates the policy is applied to a Tuxedo application. 0 indicate the policy is not applied.
COMMENTS	Comment string

Notes: Typically, you do not need to edit the policy set definition file. It is only referenced for special usage (for example, using a policy set definition to be generated with third party software).

Define a Monitoring Policy Set

Clicking **Create**, **Edit**, or **Clone** displays the Policy Set Definition page. [Table 1-7](#) lists the Policy Set Definition page properties.

Monitoring Policy Set Entry Management

Table 1-7 Monitoring Policy Set Entry Page

Name	Description
Monitoring Policy Set	Displays current policy set information
Name	Name of the policy set. Name is required for “ Create ” and “ Clone ”. “ Edit ” does not allow name change.
Description	General policy set description
Overwrite Existing Policy Set	By default, “ Create ” and “ Clone ” fail if a policy set exists with the same name. Selecting this check box allows an existing file to be overwritten.
Save	Saves current policy set changes. When policy set contents change, the save button is highlighted. If a policy set is closed before saving changes, the changes are lost.
Back	Returns to the Policy Management page
New	Creates a new policy

Table 1-7 Monitoring Policy Set Entry Page

Name	Description
Edit	Edit a selected policy. Only one policy can be selected for editing at a time.
Enable	Initiates policy setting for Tuxedo components. If a policy is already “Enabled” , no action is performed.
Disable	Disables monitoring of a Tuxedo component. Cancels all monitoring settings even if the same component is covered by other Policy Management entries.
Delete	Deletes the selected policy set.
No.	The sequence of a policy in current policy set. It is auto-increased when a new policy is added.
Latest Action	Displays the policy set status. “Enabled” indicates the policy has been successfully applied to a Tuxedo application. “Disabled” indicates the policy is not applied a Tuxedo application.
Tuxedo Component	<p>Specifies the Tuxedo component that the policy applies to.</p> <p>For example, <code>Domain[TUXDOM1]/Machine[windows]/Group[APPGRP]/Server[simpserv:1]</code> indicates the following:</p> <ul style="list-style-type: none"> • Tuxedo domain “TUXDOM1” • Machine “windows” • Group “APPGRP” • application server “simpserv” • server ID “1” <p>“Any” indicates all sub-elements of the component are selected. It is generated by the Tuxedo Object Selection panel</p>
Specification	<p>The TMMONITOR specification string for this policy. It is generated by the Policy Management Definition panel.</p> <p>For more information, see Using TSAM Agent in the <i>Tuxedo System and Application Monitor (TSAM) User's Guide</i>.</p>

Define a Policy

To define a policy, do the following steps:

1. Select the Tuxedo component to be monitored
2. Select the monitoring policy for the selected Tuxedo component

The Policy Definition page consists of the Tuxedo Component section and the Policy Management Definition section.

[Table 1-8](#) lists the Tuxedo Component properties.

Table 1-8 Tuxedo Component

Name	Description
Domain	Lists the current available Tuxedo domains. Only one domain can be selected per policy.
Machine	Lists the current available machines in the selected Tuxedo domain. “ Any ” indicates that all the machines in the domain are candidates for monitoring control.
Group	Lists the current available groups for a selected machine. “ Any ” indicates all available groups in this domain are listed.
Server	Lists the current available servers in the selected group. A specific server only can be selected when a particular group is selected. The server format is “server name:server id”.

The Policy Management Definition page allows you to select the Tuxedo application type to want to monitor. There are four Tuxedo application types:

- [Call Path](#)
- [Service](#)
- [System Server](#)
- [Transaction](#)

[Table 1-9](#) lists the Policy Management Definition properties.

Table 1-9 Policy Management Definition

Name	Description
Enable Check box	Click any or all of the four application check boxes to enable a specific application for monitoring.
Call Path Ratio	The TMMONITOR “appratio” policy. 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.
Call Path Interval	The TMMONITOR “appinterval” policy. It accepts a value range of 0-65535. It indicates a period of time (in seconds) that monitoring can be started. It is exclusive of ratio settings. The default value is “0” indicating that a time interval does not take effect.
Call Path No Log	Click this check box to enable the TMMONITOR “appnolog”. The purpose of this policy is to reduce the overhead cause by monitoring at maximum level. <code>tpgetcallinfo()</code> can still be used to retrieve monitoring information.
Call Path Bridge Decode	Click this check box to enable the BRIDGE process involved in the call path monitoring. By default, BRIDGE will not decode the application message. If this policy is specified, BRIDGE decodes the application message and log the performance metrics. Note: If the network load is heavy, BRIDGE performance is significantly affected.
Service Ratio	The TMMONITOR “svcratio” policy. It accepts a value of 1-65535. The default value is “1” indicating each service invocation is monitored.
Service Interval	The TMMONITOR “svcinterval”. It accepts a value of 0 - 65535. It indicates a period of time (in seconds) that monitoring can be started. It is exclusive of ratio settings. The default value is “0” indicating that a time interval does not take effect.

Table 1-9 Policy Management Definition

Name	Description
System Server Interval	The system server monitoring data collection interval (in seconds). It accepts a value of 30-65535. The default value is “300” indicating that for every 300 seconds, data collection occurs in the monitored system servers.
Transaction Ratio	The TMMONITOR “tranratio” policy. It accepts a value of 1-65535. The default value is “1” indicating that every Transaction routine is monitored. Note: To guarantee a complete transaction trace, we do not recommend changing the default value

For more information, see [Using TSAM Agent](#) in the *Tuxedo System and Application Monitor (TSAM) User's Guide*.

When you have completed your Policy Definition page selection, click **Save** for your selections to take effect.

Table 1-10 Save Entry and Comments

Name	Description
Save	Saves the selected policy to the current policy set. The new policy is disabled by default
Comments	Adds a comment to the policy

Import a Policy Set from Local Desktop

Click the **Import** button. The Import Policy page is displayed.

[Table 1-11](#) lists the Import Policy page properties.

Table 1-11 Import Policy Page

Name	Description
File Name	The file name on local desktop
Browser...	Browse for a file on the local desktop

Table 1-11 Import Policy Page

Name	Description
Overwrite	Click this checkbox to overwrite the policy set with imported file with the same name. By default, the uploaded file is not accepted if a policy set with the same name already exists.
Upload	Uploads the file from the desktop.
Close	Closes the import panel.

Note: If an invalid policy set file is uploaded, an error message is displayed.

Monitoring Policy Set Limitations

- TSAM does not check for Tuxedo component entries that overlap in the same or different policy set. Policy sets are applied to Tuxedo components in the order they are created.
- Disabling a Tuxedo component policy also disables all other policy settings for that Tuxedo component.
- Since TMMONITOR is also a mechanism that can be used to control monitoring behavior, TSAM does not guarantee consistency between TSAM monitoring policy settings and TMMONITOR settings.

For more information, see [Using TSAM Agent](#) in the *Tuxedo System and Application Monitor (TSAM) User's Guide*.

Tuxedo Configuration

Tuxedo Configuration allows you to view and refresh Tuxedo domain configuration information. If TSAM is running, Tuxedo configuration information is received from the LMS at boot time.

Note: If TSAM is not running at boot time, or when there are Tuxedo-side configuration changes, you must manually retrieve the configuration information.

[Table 1-12](#) lists the Tuxedo Configuration page properties.

Table 1-12 Tuxedo Configuration Page

Name	Description
Domains	Lists of Tuxedo domains in the following format: <DOMAINID>:<master machine name>:<IPCKEY>. <DOMAINID> and <IPCKEY> are configured in the UBBCONFIG *RESOURCE section; <master machine name> is configured in the UBBCONFIG *MACHINE section.
View	Displays a visible representation of the domain.
Refresh	Manually retrieves the selected domain configuration information
Expand Tree	Displays the following detailed Tuxedo domain information: Domain ID (DOMAINID), Logical Machine ID (LMID), Group name and group number (GRPNO), Server name, server ID (SRVID)
Show service	Lists the services provided by a given server.

View Tuxedo Domain Configuration

To view domain configuration information, do the following steps:

1. Select a domain from the **Domains** list

Note: Press and hold the CTRL key to select multiple domains

Some servers (including TMS, BRIDGE) that are not configured in UBBCONFIG may be displayed.

2. Click the **View** button;
3. Click the **Expand Tree** to display detailed domain information
4. Click the **Show Service** check box to display service information

Refresh Tuxedo Domain Configuration

To refresh a domain configuration, do the following steps:

1. Select a domain from the **Domains** list

Note: Press and hold the CTRL key to select multiple domains.

Some servers (including TMS, BRIDGE) that are not configured in UBBCONFIG may be displayed.

2. Click the **Refresh** button

Any of the following possible results are displayed:

- **Successful:** The configuration information is retrieved successfully, and the configuration tree is updated.
- **Failed:** The “refresh” failed. Configuration information was not retrieved.
- **Timed out:** Configuration information was not retrieved within a given time frame.

The default timeout is 30 seconds and is configured using the “tsam.config.timeoutwithtuxedo” parameter in the TSAM `web.xml` file.

Data Management

Data Management purges TSAM monitoring database. Data purge options are as follows:

- [Purge Tuxedo Component/Server/Service Data](#)
- [Purge Call Path/ Transaction Data](#)
- [Purge All Data](#)

Purge Tuxedo Component/Server/Service Data

Purge Tuxedo Component/Server/Service Data purges data based on the Tuxedo Component. [Table 1-13](#) lists the **Purge Tuxedo Component/Server/Service Data** properties.

Table 1-13 Purge Tuxedo Component/Server/Service Data

Name	Description
From	Start time [DD MM YYYY HH MM]
To	End time [DD MM YYYY HH MM]

Table 1-13 Purge Tuxedo Component/Server/Service Data

Name	Description
Scope	Purge Scope: <ul style="list-style-type: none"> • Tuxedo Component: Purges Tuxedo component and all relative data • Server Monitor: Purges Server Monitor data • Service Monitor: Purges Service Monitor Data
Domain	Domain name
Machine	Machine name
Group	Group name
Server	Server <ul style="list-style-type: none"> • Server Available: Lists all available servers • Server Selected: Lists server(s) selected for purge • Fast Search (Left/Right): Input partial server name, the cursor highlights the first matched server name
Service	Service <ul style="list-style-type: none"> • Service Available: Lists all available services • Service Selected: Lists service(s) selected for purge • Fast Search (Left/Right): Input partial service name, the cursor highlights the first matched service name

Purge Tuxedo Component/Server/Service Data

To Purge Tuxedo Component/Server/Service Data, do the following steps:

1. Select **From** and **To** for purge time period
2. Click the **Scope** check box. If a scope is not selected, data cannot be purged.
 - **Tuxedo Component:** Purge the Tuxedo Component data and its database data

Note: When **Tuxedo Component** is selected, **From** and **To** are ignored.

- **Server Monitor Data:** Purge Server Monitor data from database, but not the Tuxedo Component
- **Service Monitor Data:** Purge Service Monitor data from database, but not the Tuxedo Component

3. Select any of the following and click **Purge**.

- a. **Domain:** Select a domain and click purge. If Tuxedo Component scope is selected, the purge deletes the domain from the database and all the Machine, Group, Server, Service data under this domain.

If Tuxedo Component scope is not selected, the Server Monitor Data is automatically selected, all the Server Monitor Data under the domain is deleted. If Service Monitor data is selected, all the Service Monitor data under the domain is deleted.

- b. **Machine:** Select a machine for the domain
- c. **Group:** Select a group for the domain
- d. **Server:** Select a server for the domain
- e. **Service:** Select a service for the domain

Notes: If a **Domain** is selected, all the servers and services are populated to the **Server Available** list and **Service Available** list respectively. Use the > (single selection) or >> (all) button to add to the selected list. The **Purge** button only applies to the servers or services in the selected list.

Fast Search (Left/Right) helps to quickly locate a server or service.

Purge Call Path/ Transaction Data

Purge Call Path/ Transaction Data purges Call Path/ Transaction monitoring data. [Table 1-14](#) lists the **Purge Call Path/ Transaction Data** properties.

Table 1-14 Purge Call Path/ Transaction Data

Name	Description
From	Start time [DD MM YYYY HH MM] of time period

Table 1-14 Purge Call Path/ Transaction Data

Name	Description
To	End time [DD MM YYYY HH MM] of time period
Call Path/ Transaction	Call Path/ Transaction purges the following monitoring data: <ul style="list-style-type: none">• Call Path• Transaction

Purge Call Path/ Transaction Data

Call Path and Transaction monitoring data is independent of the Tuxedo Component.

To purge Call Path/ Transaction data, do the following steps:

1. Select purge time period by **From** and **To**
2. Click the check box for **Call Path** or **Transaction**
3. Click the **Purge** button to delete the monitoring data for Call Path/ Transaction from the database

Purge All Data

Purge All Data purges all monitoring data in **Purge Tuxedo Component/Server/Service Data** and **Purge Call Path/ Transaction Data**.

Purge All Data

Click **Purge All** to clean all the monitoring data from database, include Tuxedo Component and Call Path/ Transaction.

Notes: Only the super-user admin can purge the monitoring data.

Using any of the purge options removes monitoring data from the database. Sessions that are already logged-in are reminded to logout and re-log on to avoid data inconsistencies.

See Also

- [User Management](#)

Call Path

[Call Path Tree](#)

[Call Pattern](#)

Call Path Tree

The **Call Path Tree** Page displays Tuxedo call path application request information when Application Monitoring is turned on.

When Application Monitoring is turned on, Tuxedo associates each call path request with a unique ID name (Correlation ID). The Correlation ID denotes where the request originated and remains unchanged when the request travels across Tuxedo.

A 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. For more information, see [Table 1-12](#).
- Logical Machine ID: `LMID` in the `UBBCONFIG *MACHINES` section
- Process Name:
 - “client”: used for native 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)

Correlation ID Example

```
TUXEDO SITE1 client 13753 1 145.
```

[Table 1-15](#) lists the Call Path Tree page properties.

Table 1-15 Call Path Tree

Name	Description
Query By Correlation ID	Searches call path information for given complete Correlation ID.
Filter	Selects specific search criteria.
Enable Paging	Lists found Correlation IDs.
Rows per page	Enter number of rows to display per page.
Initiator	Performs search based on domain, node, server, or client name.

Display Correlation ID Call Path Information

To display correlation ID call path information, do the following steps:

1. Fill in the **Correlation ID** under **Query By Correlation ID**.
2. Click the **Query** button to the right of the **Correlation ID** field.

The Correlation ID table appears.

Display Calls from an Initiator with Conditions

To display calls from an initiator with conditions, do the following steps:

1. Clear **Correlation ID** if it is not empty
2. *(Optional)* Fill in the **Initiator** information under “Initiator” (Domain, Node and the Process Name)
3. Fill in **Filter** information if you want to limit the scope of the result. You can:
 - a. specify **Root Service** to display calls for a particular service
 - b. specify **Min Active Time** to display calls started for the time the service is active
 - c. Specify the search scope by using:
 - **Active Call Path**: search for unfinished call paths
 - **Call Path for latest**: search for call paths started no earlier than <n> minutes ago.
A 0 value indicates search all call paths.




- **Call Path during:** search for call path started during a time period.

4. Click the **Query** button to the left of **Enable Paging** field.

The Correlation ID table appears.

[Table 1-16](#) lists the Correlation ID Table properties

Table 1-16 Correlation ID Table

Name	Description
No.	Sequence number. Starts at 1.
Correlation ID	The Correlation ID associated with the request.
Service	The service name invoked by the initiator.
Start Time	The time the request starts. The format is ‘YY/MM/DD hh:mm:ss:SSS’ (SSS is millisecond).
Execution Time	Time elapsed (in seconds) since the request is sent out and the reply is returned.
Status	<div> Indicates finished request.</div> <div> Indicates pending request.</div> <div> Indicates failed request.</div>
Return Code	Displays a string representation and the <code>tperrno</code> value for the finished request. The display content is “TPOK/0” when there is no error.
GTRID	Displays the Global Transaction ID associated with the request, if any.

Clicking on the table column header will sort the table according to the selected column.

Clicking a **Correlation ID** displays more detailed request processing information. This detailed information is displayed in three sections:

- [Call Path Tree](#)
- [Transport Detail Table](#)
- [Service Summary Table](#)

Call Path Tree

Tuxedo request and reply are sent by the IPC message queue, or the network when the source and target are on different machine. The Call Path Tree lists the request originator (process name and PID), the Correlation ID (as its root), and the invoked service as its only child.

When you click on a Call Path Tree child, the Transport Detail table appears. [Table 1-17](#) lists the Transport Detail table properties.

You can also display the server name, the physical message queue ID and logical queue name, and/or the server location information by clicking the corresponding check box (**show server name**, **show queue info**, **show location**).

Note: A Call Path Tree child may also contain children if it makes calls when handling the request.

Transport Detail Table

A sequence number is displayed at the beginning of the service node of the Call Path Tree. [Table 1-17](#) lists the Transport Detail table properties.

Table 1-17 Transport Detail Table

Name	Description
No.	Sequence number. Starts at 1.
From	The requesting application. It consists of following fields separated by a space: DOMAINID:<hostname>:<IPCKEY>, LMID, Process Name, Server ID (SRVID in UBBCONFIG if it is a server), and PID
To	The sending application. It has the same format as “From” column.

Table 1-17 Transport Detail Table

Name	Description
Start Time	The time when this transport is begin in ‘YY/MM/DD hh:mm:ss:SSS’ format. (SSS is millisecond)
Elapsed Time	Seconds spent on this transport.
Description	Description about the transport. It denotes the type of this transport (IPC queue or network) and the type of message (request or reply).

Service Summary Table

A sequence number is displayed at the beginning of the service node of the Call Path Tree.

[Table 1-18](#) lists the Service Summary table properties.

Table 1-18 Service Summary Table



Name	Description
No.	Sequence number. The number is also shown in the beginning of invoked service in the Call Path Tree.
From	The requesting application. It consists of following fields separated by space: DOMAINID, LMID, Process Name, Server ID (SRVID in UBBCONFIG) if it's server, and PID. DOMAINID is not shown for simplicity if its value is the same as of the initiator's.
To	The sending application. It has the same format as “From” column.
Status	<div>  </div> <p>Indicates finished requests.</p> <div>  </div> <p>Indicates pending requests.</p>
Wait Time	Time elapsed (in seconds) from the time the request is sent until the time when it starts to be processed.

Table 1-18 Service Summary Table

Name	Description
Exec Time	Time elapsed (in seconds) from the time the request is sent until the time the reply is returned.
GTRID	Global Transaction ID associated when the request is processed, if called in transaction mode or if AUTOTRAN is enabled.

Clicking the GTRID field in displays the Transaction Query page.

Configure Call Information Cache

All Calls Information started after TSAM booted is cached with 100000 (**tsam.config.maxappsize**) as the default cache size (call path number of). A call path will be removed from cache if it is not finished within 600 seconds (**tsam.config.maxappactive**); otherwise it stays in cache for another 300 seconds (**tsam.config.maxappdone**) .

The parameters are configurable in the TSAM `web.xml` file.

[Table 1-19](#) list the Call Information Cache configuration parameters.

Table 1-19 Call Information Cache Configuration Parameters

Name	Description
tsam.config.maxappsize	Max number in cache for a monitored application request. Default value: 10000.
tsam.config.maxappactive	Max cache time (in seconds) for monitored application request in active status. Default value: 3600.
tsam.config.maxappdone	Max cache time (in seconds) for monitored application request in done status. Default value: 3600.

See Also

- [Query](#)

Call Pattern

Each Tuxedo call triggers a set of service invocations. The back-end service operation is transparent to the caller. It may be a local service, remote host, and even a remote domain. A challenge for application monitoring is figuring out the exact call path tree (focusing on services). One type of service invocation tree is called a pattern. TSAM provides the capability to summarize a call pattern using collected performance data.

Define the Query Conditions

The call pattern statistics is a computing and database intensive task. TSAM gives query conditions as many as possible to limit the time used on pattern computing.

Table 1-20 Items in Filter

Name	Description
Root Service	The service name of the first service invoked by the monitored request. It can only be selected when Domain is selected of Initiator panel.
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 small number of calls. The default value is 100.
Request Only	The pattern is decided by the request message. The reply messages can be dropped to reduce the time used. Reply transportation statistics are lost.
Time Window	The From and To enable the query window to second level. The default setting is the last day

Click Submit.

Note: This is a time intensive process. While you wait for results, you can continue with other monitoring tasks.

Table 1-21 Initiator Items

Name	Description
Domain	Select the domain in which the initial request started
Machine	Select the machine in which the initial request started.

Table 1-21 Initiator Items

Server	If a monitored request is started from a server, the server name can be selected to limit the query scope.
Client	If a monitored request is started from a client, the client name can be selected to limit the query scope. For more information, see Using TSAM Agent in the <i>Tuxedo System and Application Monitor (TSAM) User's Guide</i>

Pattern Query Result

Table 1-22 Pattern Result

Name	Description
Number of Patterns	How many patterns were found
Pattern Description	A simple string indicates the pattern. By clicking it can see the pattern tree.
Number of Requests	How many requests contained in this call pattern
Pattern Tree	The pattern tree is service focus and the nodes are the services name involved in this pattern. The root node is always “ INITIATOR ”. Click the Expand Tree button to expand the tree node.
Service on Pattern Tree	Click each service on pattern tree the transportation statistics to this service will be displayed
Average Transportation Time	The time (millisecond) is computed with all the requests contained in this pattern
Transportation Description	The transportation to a service might have following type: <ul style="list-style-type: none"> • IPC Queue (Request) • IPC Queue(Reply) • Network (Request) • Network (Reply)

Get Pattern with Selected Conditions

1. Input **Filter** conditions, such as root service, time window etc.
2. Limit **Initiator** scope. Select the wanted domain, machine, server or client.
3. Click the Submit button to get pattern information.
4. When the pattern tree is generated click **Initiator** to expand all tree nodes.
5. Click each service to see service transportation statistics.

See Also

- [Call Path Tree](#)

Service

[Service Monitoring](#)

[Service Historical Data Query](#)

Service Monitoring

Service Monitoring provides a visual representation of the total number of successful and failed executions for selected services on a particular Tuxedo domain. The monitoring results are displayed in a chart which can be refreshed in specific time intervals (seconds).

[Table 1-23](#) lists the Service Monitoring page properties.

Table 1-23 Service Monitoring Page

Name	Description
Domain	Domain name
Machine	Machine that the service run on
Group	Group name
Server	Server name
Most Active	Lists most active services
Time Window	Time span to aggregate the active services' success and failure number

Table 1-23 Service Monitoring Page

Name	Description
Service Available	Lists available services
Service Selected	lists selected services
Fast Search (Left)	Input any characters, then any matched service in Service Available will be highlighted.
Fast Search (Right)	Input any characters, then any matched service in Service Selected will be highlighted.

Initiate Service Monitoring

To initiate service monitoring, do the following steps:

1. Select a domain from the **Domain** drop down list. When a domain is selected, the service(s) for the domain appear in the **Service Available** drop down list.

For more specific Domain information, you can also select information from the **Machine**, **Group**, **Server** drop down lists. The default for each list is **ANY**, which indicates that all services are included.

2. There are two options for selecting services:
 - a. Select service(s) from **Service Available** to **Service Selected**. Use “>” to select individual services, or “>>” button for the entire list of services.

Note: When the Service Selected drop down list is populated, the **Most Active** drop down list is disabled.

- b. Select a number of top services from the **Most Active drop** down list.
3. Select **Time Interval**
 4. Click **Submit**. The live monitoring chart appears.
 5. Click the refresh time interval check box above the chart to periodically refresh the chart.

The chart displays the total number of successful and failed execution of services in given **time frame**. The X-axis displays the service name. The Y-axis displays the number of requests handled.

See Also

- [Service Historical Data Query](#)

Service Historical Data Query

Service Historical Data Query provides a visual representation of the statistical information for an individual service. The monitoring results are displayed in a chart.

[Table 1-24](#) lists the Service Historical Data Query page properties.

Table 1-24 Service Historical Data Query Page

Name	Description
Domain	Domain
Machine	Machine
Group	Group
Server	Server
Time Interval	Time span to aggregate the services' success and failure number
Service	Service
From	Start time (DD MM YYYY HH MM) of time period
To	End time (DD MM YYYY HH MM) of time period
Fast Search	Input any characters, then any matched service in Service will be highlighted.

Initiate Service Historical Data Query Monitoring

To initiate service historical data query monitoring, do the following steps:

1. Select a domain from the **Domain** drop down list. When a domain is selected, the service(s) for the domain appear in the **Service Available** drop down list.

For more specific Domain information, you can also select information from the **Machine**, **Group**, **Server** drop down lists. The default for each list is **ANY**, which indicates that all services are included.

2. Select **Time Interval**

3. Select time period by **From** and **To**
4. Click **Submit**. The live monitoring chart appears.

Note: **Submit** button is enabled only if a service is selected.

The chart displays the execution summary for a given service during specified time intervals. The X-axis displays the time interval. The Y-axis displays number of executions in three areas: succeeded, failed and total invoking number.

Average Execution Time and Average Wait Time are also shown in the table below the chart.

See Also

- [Server Monitoring](#)

System Server

[Server Monitoring](#)

[Server Historical Data Query](#)

Server Monitoring

Server Monitoring displays the Sever Live Monitoring information for the Tuxedo server, which includes the server snap and throughput for the given time period.

[Table 1-25](#) lists the Server Monitoring page properties.

Table 1-25 Server Monitoring Page

Name	Description
Domain	Domain name
Machine	Machine name
Group	Group name
Server	Server name.
Note: Presently, only GWTDOMAIN and BRIDGE system servers are supported.	

Table 1-25 Server Monitoring Page

Name	Description
Available Remote Domains or Hosts	If the selected server is GWTDOMAIN, then it lists all Available Remote Domains under this selected server. If the selected server is BRIDGE, then it lists all Available Remote Hosts under this selected server.
Time Window	Time Window

Initiate Server Monitoring

To initiate server monitoring, do the following steps:

1. Make a selection from each of the following drop-down lists: **Domain, Machine, Group, Server**: Available remote domains and hosts are shown in the **Available Remote Domains or Hosts** drop-down list.
2. Make a selection from the **Available Remote Domains or Hosts** drop-down list.
By default, all remote domains or hosts are selected.
3. Select **Time Interval**
4. Click **Submit**. The server statistics chart appears.

Note: The **Submit** button is enabled only when the **Available Remote Domains or Hosts** drop-down list is populated.

Note: To periodically refresh the chart, click the refresh time interval checkbox.

Server Monitoring charts display server information during specified time intervals. The **Snapshot** chart displays statistic data at sampling moment. The **Throughput** chart displays accumulated statistical data over a period of time.

The X-axis display the time. The **Snapshot** chart Y-axis displays the number of outstanding requests for GWTDOMAIN, or the number of messages queued for the BRIDGE remote host. The **Throughput** chart Y-axis displays the number of messages sent to the remote domain or remote host.

See Also

- [Server Historical Data Query](#)

Server Historical Data Query

Server Historical Data Query page displays Tuxedo server statistical information. [Table 1-26](#) list the Server Historical Data Query page properties.

Table 1-26 Server Historical Data Query Page

Name	Description
Domain	Domain
Machine	Machine
Group	Group
Server	Server
Available Remote Domains or Hosts	If the selected server is GWTDOMAIN, then it lists all Available Remote Domains under this selected server. If the selected server is BRIDGE, then it lists all Available Remote Hosts under this selected server.
Time Interval	Time span (minutes)
From	Start time (DD MM YYYY HH MM) of time period
To	End time (DD MM YYYY HH MM) of time period

[Table 1-27](#) lists the Snapshot and Throughput page properties.

Table 1-27 Snapshot and Throughput Page

Name	Item	Description
	When	Time period.
Snapshot	MsgNum	Number of messages go through in the sampling moment.
	MsgSize	Total number of messages' size in the sampling moment.
	WaitReply#	Number of pending requests waiting for reply in the sampling moment.

Table 1-27 Snapshot and Throughput Page

Throughput	MsgNum	Accumulated number of messages go through in the sampling period.
	MsgSize	Accumulated number of messages' size in the sampling period.

Initiate Server Historical Data Query

To initiate a server historical data query, do the following steps:

1. Make a selection from each of the following drop-down lists: **Domain**, **Machine**, **Group**, **Server**: Available remote domains and hosts are shown in the **Available Remote Domains or Hosts** drop-down list.
2. Make a selection from the **Available Remote Domains or Hosts** drop-down list.
By default, all remote domains or hosts are selected.
3. Select **Time Interval**
4. Select time period by **From** and **To**
5. Click **Submit**. The server statistics chart appears.

Note: **Submit** button is enabled only when the **Available Remote Domains or Hosts** drop-down list is populated.

The **Server Historical Data Query** chart displays throughput data for given server for a specific time period. The X-axis displays the time. The Y-axis displays the accumulated number of message during a specified **Time Interval**.

See Also

- [Server Monitoring](#)

Transaction

Query

Query

.Transaction Query page allows you to search for and display transaction information.

There are three ways to initiate a transaction query:




- specify partial or complete Global Transaction ID (GTRID) for specific transaction
- specify the earliest time when the transaction was started
- specify both GTRID and time

Clicking submit displays a GTRID general information table. [Table 1-28](#) list the GTRID general information properties.

Table 1-28 GRTRID General Information Page

Name	Description
No.	Sequence number. Starts at 1.
Initiator	Transaction initiator. Consists of the value of following fields separated by a space: <ol style="list-style-type: none"> <DOMAINID>:<master address>:<IPCKEY>(see Table 1-12) Machine ID (LMID in UBBCONFIG's *MACHINES section) Group Name, server only Process Name Server ID (SRVID in UBBCONFIG's *SERVERS section), server only Process ID (pid).
GTRID	Global Transaction ID.

Table 1-28 GRTRID General Information Page

Status	 Indicates finished request.  Indicates pending request.  Indicates failed request.
Start Time	Transaction starting time in the format of 'YY/MM/DD hh:mm:ss:SSS', where SSS stands for milliseconds.
Duration	Transaction life time
Exec Time	Total time elapsed for all Transaction operations.
Parent GTRID	denote original GTRID for transaction across Tuxedo domain.

Note: Click on any of the column headings to sort in ascending or descending order.

Clicking on a GTRID displays three additional tables:

- Transaction Participant(s)

Displays which group join this transaction and particular, which servers (process name, server ID and pid) in that group is participating.

- Involved Call Correlation ID(s)

Provides a link that lists Call Correlation ID(s) executed under a transaction for a specific server.

- Transaction Detail

[Table 1-29](#) lists the Transaction Detail page properties.

Table 1-29 Transaction Detail Information

Name	Description
No.	Sequence number. Starts at 1.
Location	where Transaction operation occurred in the same format as “Initiator” in brief table.
XA OP	Transaction operation name.
Retcode	Transaction operation return code.
Start Time	Transaction operation starting time in format of ‘YY/MM/DD hh:mm:ss:SSS’, where SSS stands for milliseconds.
Exec Time	Seconds elapsed for given Transaction operation.

Query Transaction information for a Specific GTRID

To query transaction information for a specific GTRID, do the following steps:

1. Enter **GTRID** value. Check **Exact Match** if partial GTRID entered.
Note: When **Exact Match** is not checked, all transactions that include a **GTRID** are shown.
2. Reset **Time Window** to zero if you are not sure when the transaction started.
3. Click the **Submit** or **Refresh** button;
4. Click the **GTRID** to display more information.

Query All Past Transactions

To query all past transaction, do the following steps

1. Clear **GTRID** if it is not empty.
2. Enter the time interval in the **Time Window** to specify the earliest started transaction.
3. Click the **Submit** or **Refresh** button.
4. Click a **GTRID** to display more information.

Get GTRID Call information

To get GTRID call information, do the following steps:

1. Enter search information and click the **Submit** or **Refresh** button;
2. Click on a **GTRID** link under the **GTRID** column.
3. Click the link in the column next to **Involved Calls Correlation ID(s)**. The **Call Path Tree** query page appears.

Note: The “INFO: nothing found” error message may appear due to the following:

- a. The call was started before TSAM server started
- b. The call information was discarded due to the Call Path Information retire policy.

See Also

- [Call Path Tree](#)

Alerts

[Alert Management](#)

[Events](#)

Alert Management

The **Alert Management** page lists current TSAM alerts. It allows you to “**Add**”, “**Edit**” and “**Delete**” TSAM alerts. [Table 1-30](#) lists the Alert Management page properties.

Table 1-30 Alert Management Page

Name	Description
Name	Alert name. Must be given when this alert is created.
Type	Alert type. TSAM supports four alert types: “Application”, “Service”, “System” and “Transaction” which correspond to the four performance monitoring categories.
Description	Alert description.
Add	Add a new alert

Table 1-30 Alert Management Page

Edit	Edit a selected alert
Delete	Delete selected alert(s)

Alert Definition

The **Alert Definition** page appears when you click the “**Add**” or “**Edit**” button.

Note: “**Edit**” displays the settings of the selected alert. The name and type cannot be changed.

[Table 1-31](#) lists the Alert Definition page properties.

Table 1-31 Alert Definition Page

Name	Description
Alert Name	Name of the alert. Must be given in order to create an alert
Alert Type	The type of alert to be created. Four types are supported: <ul style="list-style-type: none">• Call Path: For application monitoring related alerts• Service: For service monitoring related alerts• System: For system server monitoring related alerts• Transaction: For transaction monitoring related alerts

Table 1-31 Alert Definition Page

Alert Definition	<p>Defines the items that generate an event. They are alert-type specific.</p> <p>Application Type:</p> <ul style="list-style-type: none"> • Elapse time. The time elapsed since this request monitored. The event will be generated once the time threshold is reached. The unit is second. • IPC Queue Length. The request IPC queue length on the call path tree of this monitored request. It is an integer threshold and events will be generated if any request queue length exceeds the defined value. • Execution Error. It is a boolean threshold that events will be generated when Tuxedo service execution encounters error <p>Service Type</p> <ul style="list-style-type: none"> • Execution time. The elapsed execution time for a service. The event will be generated once the time threshold is reached. The unit is second. • IPC Queue Length. The request IPC queue length monitored application service. It is an integer threshold and events will be generated if the queue length exceeds the defined value. • Execution Error. It is a boolean threshold that events will be generated when Tuxedo service execution encounters error <p>System Type</p> <ul style="list-style-type: none"> • Network Link Lost. An event will be generated when a network link was lost <p>Transaction Type</p> <ul style="list-style-type: none"> • Transaction Call Failure. A Transaction call failure will result an event generation
Severity	<p>Four security levels can be selected:</p> <ul style="list-style-type: none"> • Information • Warn • Critical • Fatal
Action	<p>The action defines which action need to be performed when the evaluation is true if the alert. Current only Tuxedo Event is supported. When Tuxedo Event is selected, Tuxedo Event Name and Tuxedo Event Message must be supplied.</p>
Description	A description string for this alert

See Also

- [Event Query](#)

Events

The **Events** page displays alerts and details generated based on alert conditions you create in the **Alert Management** page. The **Show All Events** button lists all the events. The **Filter Events** button shows the filter conditions panel above. **Submit** button lists events based on the filter condition; while **Hide** button hides filter conditions panel.

Table 1-32 Events Page

Name	Description
Show All Events	Lists all the Events in detail
Filter Events	Lists all Event details based on the filter condition
Show XX Events per Page	Displays the selected number of Events per page.

Table 1-33 Filter Conditions Panel

Name	Description
Event Name	Event name
Event Type	Event Type <ul style="list-style-type: none"> • Call Path • Service • System • Transaction

Table 1-33 Filter Conditions Panel

Name	Description
Event Severity	Event Severity <ul style="list-style-type: none"> • Information • Warning • Critical • Fatal while Information is lowest, Fatal is highest.
Include and below	If checked, all events listed under Event Severity and below are included. If unchecked, only the events under this Event Severity.
From	Start time (DD MM YYYY HH MM) of time period
To	End time (DD MM YYYY HH MM) of time period
Submit	Lists all Event details based on the filter condition
Hide	Hide the filter conditions panel

[Table 1-34](#) lists the Event Details page properties.

Table 1-34 Events Detail Page

Name	Description
Report Time	Event log time at TSAM
Name	Event Name created at Alert Management page
Type	Event Type create at Alert Management page
Severity	Event Severity create at Alert Management page
Description	Event Description create at Alert Management page

Delete Events button, at the bottom of the whole page, is to delete events.

Show All Events

Click the **Show All Events** button to list all events.

Filter Events

To filter events, do the following steps:

1. Click **Filter Events** button to show the filter conditions panel above;
1. Select the Event Name, Event Type, Event Severity, and time period (From, To);
2. Click **Submit** button. The events matching the filter conditions are listed;
3. Click **Hide** button to hide the filter conditions panel above.

Note: If only show the exact severity events, make Include and below check box off; if you'd like to show all the event at severity and below, make Include and below on.

Delete Events

To delete events, do the following steps:

1. Select event by click the check box at first column at every event on the left, or click the check box on the head left to select all events on current page.
2. Click the Delete Events button will delete selected events. The deleted events brief information will be shown at bottom of the page.

See Also

- [Alert Management](#)

Recent Events

The bottom-left panel of the TSAM console lists a summary of generated events. Clicking any of the event types in the panel lists the events on the Recent Events page.

[Table 1-35](#) lists the Recent Events Page properties

Table 1-35 Recent Events Page

Name	Description
Alert Type	The type of alert which generated this event

Table 1-35 Recent Events Page

Severity	The severity of the source alert
Report Time	When the event was generated.
Description	Description of this event

Clean the Event in Cache

- Click **Clean** to clear all the events stored in cache. The events can also be queried by **Alerts/Events page**.

Customize the Event Cache Time

You can specify how long an event remains stored in cache. Enter the required time by changing the `tsam.config.windowevt` value in the TSAM `web.xml` file. The default value is 60 minutes.

See Also

- [Alert Management](#)
- [Events](#)