



**BEA TSAM™**

**BEA (TSAM) Console  
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 BEA TSAM console is composed of two sections:

[Monitoring Center](#): BEA TSAM administration, monitored data access, and alerts definition.

[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 BEA 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    |
|--------------------|----------------|
| <b>User Name</b>   | User name      |
| <b>Description</b> | 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 User** button to add a new user. The **Add New User** page appears.

**Note:** Only the 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            |
|------------------|------------------------|
| <b>User Name</b> | New user name [4..15]  |
| <b>Password</b>  | Enter password [4..15] |

**Table 1-2 Add New User Page**

| <b>Name</b>             | <b>Description</b>        |
|-------------------------|---------------------------|
| <b>Confirm Password</b> | Re-enter password [4..15] |
| <b>Description</b>      | Describes user [0..50]    |

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:** Users can only change their respective password.

Only the super-user admin can change all user passwords.

The user name and description cannot be changed.

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

**Table 1-3 Change Password Page**

| <b>Name</b>         | <b>Description</b>        |
|---------------------|---------------------------|
| <b>User Name</b>    | User name[4..15]          |
| <b>Old Password</b> | Enter old password[4..15] |
| <b>New Password</b> | Enter password[4..15]     |

**Table 1-3 Change Password Page**

| <b>Name</b>                 | <b>Description</b>       |
|-----------------------------|--------------------------|
| <b>Confirm New Password</b> | Re-enter password[4..15] |
| <b>User Description</b>     | 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 description you want to change.
2. Click the **Change Description** button.

The **Change User Description** page appears.

**Note:** Users can only change their respective description.

Only the super-user admin can change all user descriptions.

[Table 1-4](#) lists the **Change User Description** page properties.

**Table 1-4 Change User Description Page**

| <b>Name</b>             | <b>Description</b>                |
|-------------------------|-----------------------------------|
| <b>User Name</b>        | User name[4..15]                  |
| <b>User Description</b> | 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 next to the user you want to delete.
2. Click the **Delete User** button to delete users.

**Notes:** Only the super-user admin can delete users.

The super-user admin cannot be deleted.

## Policy Management

BEA 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, Export, and Delete** monitoring policies. [Table 1-5](#) lists the Monitoring Policy Sets Management page properties.

**Table 1-5 Monitoring Policy Sets Management Page**

| <b>Name</b>                   | <b>Description</b>  |
|-------------------------------|---|
| <b>Latest Used Policy Set</b> | BEA 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.   |
| <b>Available Policy Sets</b>  | BEA 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 BEA TSAM Web application file <code>tsam.config.schemesdir</code> in the <code>web.xml</code> . |
| <b>Name</b>                   | Name of the policy set.   |
| <b>Last Modified Time</b>     | Displays last time the policy set was modified.   |
| <b>Create</b>                 | Creates a new monitoring policy set.  |
| <b>Edit</b>                   | Edit an existing monitoring policy set. Only one monitoring policy can be selected at a time.   |
| <b>Clone</b>                  | 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 <b>Name</b> attributes are not copied. The latest policy action in the new policy set is disabled by default.                    |
| <b>Import</b>                 | Imports a policy set definition file from desktop and uploads to server.  |
| <b>Export</b>                 | Exports policy set information into a policy set definition file.<br><b>Note:</b> <b>Export</b> can also be performed by clicking <b>Policy Set Name</b>  |
| <b>Delete</b>                 | 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**

| <b>Element Name</b> | <b>Description</b>  |
|---------------------|---|
| <b>TSAM_POLICY</b>  | Root tag name of the policy set definition file   |
| <b>NAME</b>         | Name of policy set  |
| <b>DESCRIPTION</b>  | Policy Set description string   |
| <b>POLICY</b>       | A policy in a policy set. You can define multiple policies.   |
| <b>TUXOBJECT</b>    | Sub-element of <b>POLICY</b> . It represents which Tuxedo back end policy is impacted by the policy. Its format is:<br><pre>Domain Machine Group Server</pre> <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> |
| <b>DEFINITION</b>   | The monitoring definition string. Has the same format as TMMONITOR.<br><br>For more information, see BEA TSAM Agent, <a href="#">Monitoring Properties</a> , in the <i>Tuxedo System and Application Monitor (TSAM) Administration Guide</i> .  |
| <b>STATUS</b>       | Indicates policy status. 1 indicates the policy is applied to a Tuxedo application. 0 indicate the policy is not applied.   |
| <b>COMMENTS</b>     | 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**

| <b>Name</b>                  | <b>Description</b>   |
|------------------------------|--|
| <b>Monitoring Policy Set</b> | Displays current policy set information  |
| <b>Name</b>                  | Name of the policy set. Name is required for “ <b>Create</b> ” and “ <b>Clone</b> ”. “ <b>Edit</b> ” does not allow name change.   |
| <b>Description</b>           | General policy set description   |
| <b>Overwrite</b>             | By default, “ <b>Create</b> ” and “ <b>Clone</b> ” fail if a policy set exists with the same name. Selecting this check box allows an existing file to be overwritten.                                       |
| <b>Save</b>                  | 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.                                    |
| <b>Back</b>                  | Returns to the <b>Policy Management</b> page   |
| <b>New</b>                   | Creates a new policy   |
| <b>Edit</b>                  | Edit a selected policy. Only one policy can be selected for editing at a time.   |
| <b>Enable</b>                | Initiates policy setting for Tuxedo components. If a policy is already “ <b>Enabled</b> ”, re-apply the policy.  |
| <b>Disable</b>               | Disables monitoring of a Tuxedo component. Cancels all monitoring settings even if the same component is covered by other Policy Management entries.   |
| <b>Delete</b>                | Deletes the selected policy set.   |
| <b>No.</b>                   | The sequence of a policy in current policy set. It is auto-increased when a new policy is added.   |
| <b>Latest Action</b>         | Displays the policy set status. “ <b>Enabled</b> ” indicates the policy has been successfully applied to a Tuxedo application. “ <b>Disabled</b> ” indicates the policy is not applied a Tuxedo application. |

**Table 1-7 Monitoring Policy Set Entry Page**

| Name                    | Description  |
|-------------------------|--|
| <b>Tuxedo Component</b> | <p>Specifies the Tuxedo component that the policy applies to.</p> <p>For example,<br/> “Domain[TUXDOM1]/Machine[windows]/Group[APPGRP]/Server[simpserv:1]” indicates the following:</p> <ul style="list-style-type: none"> <li>• Tuxedo domain “TUXDOM1”</li> <li>• Machine “windows”</li> <li>• Group “APPGRP”</li> <li>• application server “simpserv”</li> <li>• server ID “1”</li> </ul> <p>“<b>Any</b>” indicates all sub-elements of the component are selected. It is generated by the <b>Tuxedo Object Selection</b> panel</p> |
| <b>Specification</b>    | <p>The TMMONITOR specification string for this policy. It is generated by the <b>Policy Management Definition</b> panel.</p> <p>For more information, see BEA TSAM Agent, <a href="#">Monitoring Properties</a>, in the <i>Tuxedo System and Application Monitor (TSAM) Administration 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**

| <b>Name</b>    | <b>Description</b>  |
|----------------|---|
| <b>Domain</b>  | Lists the current available Tuxedo domains. Only one domain can be selected per policy.   |
| <b>Machine</b> | Lists the current available machines in the selected Tuxedo domain. “ <b>Any</b> ” indicates that all the machines in the domain are candidates for monitoring control.   |
| <b>Group</b>   | Lists the current available groups for a selected machine. “ <b>Any</b> ” indicates all available groups on the node are eligible for monitoring control.   |
| <b>Server</b>  | 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”. “ <b>Any</b> ” indicates all available servers in the group are eligible for monitoring control. |

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**

| <b>Name</b>             | <b>Description</b>  |
|-------------------------|---|
| <b>Enable Check box</b> | Click any or all of the four application check boxes to enable a specific application for monitoring.   |
| <b>Call Path Ratio</b>  | 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. |

Table 1-9 Policy Management Definition

| Name                           | Description  |
|--------------------------------|--|
| <b>Call Path Interval</b>      | 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.  |
| <b>Call Path No Log</b>        | Click this check box to enable “appnolog”. For the selected component, the TMMONITOR plug-in is not invoked, that is the monitor data will not be collected.<br><br>This policy reduces the overhead caused by maximum level monitoring. <code>tpgetcallinfo()</code> can still be used to retrieve monitoring information.                              |
| <b>Call Path Bridge Decode</b> | 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.<br><br><b>Note:</b> If the network load is heavy, BRIDGE performance is significantly affected. |
| <b>Service Ratio</b>           | The TMMONITOR “svcratio” policy. It accepts a value of 1-65535. The default value is “1” indicating each service invocation is monitored.  |
| <b>Service Interval</b>        | 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.   |
| <b>System Server Interval</b>  | 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.  |
| <b>Transaction Ratio</b>       | The TMMONITOR “tranratio” policy. It accepts a value of 1-65535. The default value is “1” indicating that every Transaction routine is monitored.<br><br><b>Note:</b> To guarantee a complete transaction trace, we do not recommend changing the default value  |

For more information, see BEA TSAM Agent in the *Tuxedo System and Application Monitor (TSAM) Administration Guide*.

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

**Table 1-10 Save Entry and Comments**

| Name              | Description  |
|-------------------|--|
| <b>Add/Update</b> | Adds or updates the selected policy to the current policy set. The new policy is disabled by default |
| <b>Comments</b>   | 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  |
|-------------------|--|
| <b>File Name</b>  | The file name on local desktop   |
| <b>Browser...</b> | Browse for a file on the local desktop   |
| <b>Overwrite</b>  | Click this check box 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. |
| <b>Upload</b>     | Uploads the file from the desktop.   |
| <b>Close</b>      | Closes the import panel.   |

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

## Monitoring Policy Set Limitations

- BEA TSAM does not check for Tuxedo component entries that overlap in the same or different policy set. If multiple policies are applied at the same time, the policies 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, BEA TSAM does not guarantee consistency between BEA TSAM monitoring policy settings and TMMONITOR settings.

For more information, see BEA TSAM Agent in the *Tuxedo System and Application Monitor (TSAM) Administration Guide*.

## Tuxedo Configuration

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

**Note:** If BEA TSAM is not running at boot time, or if 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  |
|---------------------|--|
| <b>Domains</b>      | Lists Tuxedo domains in the following format:<br><DOMAINID>:<master machine name>:<IPCKEY>.<br><br><DOMAINID> and <IPCKEY> are configured in the UBBCONFIG *RESOURCE section; <master machine name> is configured in the UBBCONFIG *MACHINE section. |
| <b>View</b>         | Displays a visible representation of the domain.   |
| <b>Refresh</b>      | Manually retrieves the selected domain configuration information   |
| <b>Expand Tree</b>  | Displays the following detailed Tuxedo domain information: Domain ID (DOMAINID), Logical Machine ID (LMID) and Tuxedo version, Group name and group number (GRPNO), Server name, server ID (SRVID)   |
| <b>Show service</b> | 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 BEA TSAM `web.xml` file.

## Data Management

**Data Management** purges BEA 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**

| <b>Name</b>    | <b>Description</b>   |
|----------------|--|
| <b>From</b>    | Start time [DD MM YYYY HH MM]  |
| <b>To</b>      | End time [DD MM YYYY HH MM]  |
| <b>Scope</b>   | Purge Scope: <ul style="list-style-type: none"> <li>• Tuxedo Component: Purges Tuxedo component and all relative data</li> <li>• Server Monitor: Purges Server Monitor data</li> <li>• Service Monitor: Purges Service Monitor Data</li> </ul> |
| <b>Domain</b>  | Domain name  |
| <b>Machine</b> | Machine name   |
| <b>Group</b>   | Group name   |

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

| <b>Name</b>    | <b>Description</b>   |
|----------------|--|
| <b>Server</b>  | Server <ul style="list-style-type: none"> <li>• Server Available: Lists all available servers</li> <li>• Server Selected: Lists server(s) selected for purge</li> <li>• Fast Search (Left/Right): Input partial server name, the cursor highlights the first matched server name</li> </ul>        |
| <b>Service</b> | Service <ul style="list-style-type: none"> <li>• Service Available: Lists all available services</li> <li>• Service Selected: Lists service(s) selected for purge</li> <li>• Fast Search (Left/Right): Input partial service name, the cursor highlights the first matched service name</li> </ul> |

### **Purge Tuxedo Component/Server/Service Data**

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

1. Select **From** and **To** to enter 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 **Scope (Tuxedo Component)** is checked, **Purge** deletes the selected domain from the database and all the Machine, Group, Server, Service and their monitoring data under this domain.

If **Scope (Tuxedo Component)** is unchecked, **Scope (Server Monitor Data and Service Monitor data)** is automatically checked. If **Server Monitor Data** is checked, **Purge** deletes all the Server Monitor Data under the selected domain. If **Service Monitor data** is checked, **Purge** deletes all the Service Monitor data under the selected domain.

- b. **Machine:** same procedure as **Domain**.
- c. **Group:** same procedure as **Domain**.
- d. **Server:** same procedure as **Domain**.
- e. **Service:** same procedure as **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   |
|-----------------------------------|---|
| <b>From</b>                       | Start time [DD MM YYYY HH MM] of time period  |
| <b>To</b>                         | End time [DD MM YYYY HH MM] of time period  |
| <b>Call Path/<br/>Transaction</b> | Call Path/ Transaction purges the following monitoring data: <ul style="list-style-type: none"> <li>● Call Path</li> <li>● Transaction</li> </ul> |

## 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 **From** and **To** to enter purge time period.
2. Click the **Call Path** or **Transaction** check box.
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 monitoring data.

When you click the **Purge** button, the monitoring data is purged from the database. All other active sessions will be reminded to logout and re-login again 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
  - “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)**

### Correlation ID Example

```
TUXEDO:lcsol18:200401 SITE1 client 18505 1 1.
```

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

**Table 1-15 Call Path Tree**

| Name                           | Description   |
|--------------------------------|---|
| <b>Query By Correlation ID</b> | Searches call path information for given complete Correlation ID. |
| <b>Filter</b>                  | Selects specific search criteria.                                 |
| <b>Enable Paging</b>           | Lists found Correlation IDs.                                      |
| <b>Rows per page</b>           | Enter number of rows to display per page.                         |
| <b>Initiator</b>               | 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 (**Domain, Machine, Server** or **Client**).
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 Elapsed Time** to display calls started for the time the service is active
  - c. Specify the search scope by using the following return codes:
    - any: search all call paths regardless of return code
    - failed: search failed call paths
    - succeeded: search all successful call paths
  - d. 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. A `value(0)` 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                                     |
|-----------------------|---|
| <b>No.</b>            | Sequence number. Starts at 1.                   |
| <b>Correlation ID</b> | The Correlation ID associated with the request. |
| <b>Service</b>        | The service name invoked by the initiator.      |



Table 1-16 Correlation ID Table

| Name                  | Description   |
|-----------------------|---|
| <b>Start Time</b>     | Request start time. The format is 'YY/MM/DD hh:mm:ss:SSS' (SSS = millisecond).  |
| <b>Execution Time</b> | Time elapsed (in seconds) since the request is sent out and the reply is returned.  |
| <b>Status</b>         | <p><br/>Indicates finished request.</p> <p><br/>Indicates pending request.</p> <p><br/>Indicates failed request.</p> <p><b>Note:</b> A call path is displayed as “timed out” if it remains active for more than 10 minutes. The timeout threshold can be changed using the &lt;web.xml&gt; <code>tsam.callpath.timeout</code> parameter.</p> |
| <b>Return Code</b>    | 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.   |
| <b>GTRID</b>          | 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 call info, 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 call info, 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. A sequence number is displayed at the beginning of the service node of the Call Path Tree.

## Transport Detail Table

[Table 1-17](#) lists the Transport Detail table properties.

**Table 1-17 Transport Detail Table**

| Name              | Description   |
|-------------------|---|
| <b>No.</b>        | Sequence number. Starts at 1.   |
| <b>From</b>       | The requesting application.<br>It consists of following fields separated by a space:<br>DOMAINID: <hostname> : <IPCKEY> , LMID, Process Name, Server ID (SRVID in UBBCONFIG) if it is a server, and PID |
| <b>To</b>         | The sending application.<br>It has the same format as “From” column.  |
| <b>Start Time</b> | Transport start time. The format is ‘YY/MM/DD hh:mm:ss:SSS’ (SSS = millisecond).  |

**Table 1-17 Transport Detail Table**

| <b>Name</b>         | <b>Description</b>  |
|---------------------|---|
| <b>Elapsed Time</b> | Seconds spent on this transport.  |
| <b>Description</b>  | 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

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

**Table 1-18 Service Summary Table**

| <b>Name</b>   | <b>Description</b>  |
|---------------|---|
| <b>No.</b>    | Sequence number. The number is also shown in the beginning of invoked service in the Call Path Tree.  |
| <b>From</b>   | The requesting application.<br><br>It consists of following fields separated by a space:<br><DOMAINID>: <master machine name>: <IPCKEY>, LMID, Process Name, Server ID (SRVID in UBBCONFIG) if it is a server, and PID. |
| <b>Action</b> | Call information.   |
| <b>To</b>     | The sending application.<br><br>It has the same format as “From” column.  |

**Table 1-18 Service Summary Table**

| Name             | Description   |
|------------------|---|
| <b>Status</b>    | <br>Indicates finished request.<br><br>Indicates pending request.<br><br>Indicates failed request. |
| <b>Wait Time</b> | Time elapsed (in seconds) from the time the request is sent until the time when it starts to be processed.  |
| <b>Exec Time</b> | Time elapsed (in seconds) from the time the request is sent until the time the reply is returned.   |
| <b>GTRID</b>     | 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 call paths started after BEA TSAM boots are cached using 100000 (`tsam.config.maxappsize`) as the default cache size (number of call paths). A call paths is removed from cache if it is not finished within 600 seconds (`tsam.config.maxappactive`). If it finishes *before* 600 seconds, it remains cached for another 300 seconds (`tsam.config.maxappdone`) after it is finished.

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

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

**Table 1-19 Call Information Cache Configuration Parameters**

| <b>Name</b>                               | <b>Description</b>   |
|---|--|
| <b>tsam.conf<br/>ig.maxapp<br/>size</b>   | Max number in cache for a monitored application request.<br>Default value: 10000.                      |
| <b>tsam.conf<br/>ig.maxapp<br/>active</b> | Max cache time (in seconds) for monitored application request in active status.<br>Default value: 600. |
| <b>tsam.conf<br/>ig.maxapp<br/>done</b>   | Max cache time (in seconds) for monitored application request in done status.<br>Default value: 300.   |

## 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. BEA 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. BEA TSAM issues as many query conditions as possible to limit the time used on pattern computing.

**Table 1-20 Items in Filter**

| <b>Name</b>         | <b>Description</b>  |
|---------------------|---|
| <b>Root Service</b> | The service name of the first service invoked by the monitored request. It can only be selected when <b>Domain</b> is selected in the <b>Initiator</b> panel. |

**Table 1-20 Items in Filter**

|                               |  |
|-------------------------------|--|
| <b>Minimum Request Number</b> | 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. The default value is 100. |
| <b>Request Only</b>           | The pattern is decided by the request message. The reply messages can be dropped to reduce the time used. Reply statistics are lost.   |
| <b>Time Window</b>            | The <b>From</b> and <b>To</b> 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**

| <b>Name</b>    | <b>Description</b>  |
|----------------|---|
| <b>Domain</b>  | Select the domain in which the initial request started  |
| <b>Machine</b> | Select the machine in which the initial request started.  |
| <b>Server</b>  | If a monitored request is started from a server, the server name can be selected to limit the query scope.  |
| <b>Client</b>  | If a monitored request is started from a client, the client name can be selected to limit the query scope. For more information, see BEA TSAM Agent in the <i>Tuxedo System and Application Monitor (TSAM) Administration Guide</i> . |

## Pattern Query Result

**Table 1-22 Pattern Result**

| <b>Name</b>                | <b>Description</b>  |
|----------------------------|---|
| <b>Number of Patterns</b>  | How many patterns were found  |
| <b>Pattern Description</b> | A simple string indicates the pattern. By clicking it can see the pattern tree. |

**Table 1-22 Pattern Result**

|                                    |  |
|------------------------------------|--|
| <b>Number of Requests</b>          | How many requests contained in this call pattern   |
| <b>Pattern Tree</b>                | The pattern tree is service focus and the nodes are the services name involved in this pattern. The root node is always “ <b>INITIATOR</b> ”. Click the Expand Tree button to expand the tree node.  |
| <b>Service on Pattern Tree</b>     | Click each service on pattern tree the transportation statistics to this service will be displayed   |
| <b>Average Transportation Time</b> | The time (millisecond) is computed with all the requests contained in this pattern   |
| <b>Transportation Description</b>  | The transportation to a service might have following type: <ul style="list-style-type: none"> <li>• IPC Queue (Request)</li> <li>• IPC Queue(Reply)</li> <li>• Domain (Request)</li> <li>• Domain (Reply)</li> <li>• BRIDGE (Request)</li> <li>• BRIDGE (Reply)</li> </ul> |

## Get Pattern with Selected Conditions

1. Input **Filter** conditions, such as root service, time window etc.
2. Limit **Initiator** scope. Select **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**

| <b>Name</b>                | <b>Description</b>   |
|----------------------------|--|
| <b>Domain</b>              | Domain name  |
| <b>Machine</b>             | Machine that the service run on  |
| <b>Group</b>               | Group name   |
| <b>Server</b>              | Server name  |
| <b>Most Active</b>         | Lists most active services   |
| <b>Time Window</b>         | Time span to aggregate the active services' success and failure number                   |
| <b>Service Available</b>   | Lists available services   |
| <b>Service Selected</b>    | lists selected services  |
| <b>Fast Search (Left)</b>  | Input any characters, then any matched service in Service Available will be highlighted. |
| <b>Fast Search (Right)</b> | 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 service selection options:
  - a. Select service(s) from **Service Available** to **Service Selected**. Use “>” to select individual services, or “>>” button for the entire list of services.
  - b. Select a number of top services from the **Most Active** drop-down list.
- Note:** The max number of service that can be monitored at one time is 20.
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 service executions in a given time frame. The X-axis displays the service name. The Y-axis displays the number of requests handled during the most recent time period (in <n> minutes), where <n> is specified in the **Time Window**.

## 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 |
|----------------|-------------|
| <b>Domain</b>  | Domain      |
| <b>Machine</b> | Machine     |
| <b>Group</b>   | Group       |

**Table 1-24 Service Historical Data Query Page**

| <b>Name</b>          | <b>Description</b>  |
|----------------------|---|
| <b>Server</b>        | Server  |
| <b>Time Interval</b> | Time span to aggregate the services' success and failure number |
| <b>Service</b>       | Service   |
| <b>From</b>          | Start time (DD MM YYYY HH MM) of time period                    |
| <b>To</b>            | End time (DD MM YYYY HH MM) of time period                      |
| <b>Fast Search</b>   | Input any characters, then any matched service is 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 a service from the **Service** list box
3. Select **Time Interval**.
4. Select time period by **From** and **To**.
5. Click **Submit**. The live monitoring chart appears.

The chart displays the execution summary for a given service during the specified **From** and **To** time range. The X-axis displays the time interval. The Y-axis displays number of executions during the time interval.

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

## 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.

**Note:** Server monitoring data includes both user monitoring data *and* Tuxedo system data.

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

**Table 1-25 Server Monitoring Page**

| Name                                     | Description  |
|--|--|
| <b>Domain</b>                            | Domain name  |
| <b>Machine</b>                           | Machine name   |
| <b>Group</b>                             | Group name   |
| <b>Server</b>                            | Server name.<br><br><b>Note:</b> Presently, only GWTDOMAIN and BRIDGE system servers are supported.  |
| <b>Available Remote Domains or Hosts</b> | If the selected server is GWTDOMAIN, then it lists all <b>Available Remote Domains</b> under this selected server. If the selected server is BRIDGE, then it lists all <b>Available Remote Hosts</b> under this selected server. |
| <b>Time Window</b>                       | 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 Window**.

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 check box.

The charts display server information for the past **Time Window**. The **Snapshot** chart displays real-time sampling statistical data. The **Throughput** chart displays accumulated statistical data during a given time period.

The X-axis displays the time. [Table 1-26](#) lists the Y-axis display.

**Table 1-26 Snapshot and Throughput Y-axis Display**

| System Server | Snapshot   | Throughput  |
|---------------|--|---|
| BRIDGE        | Number of messages queued for the remote host at the time the data is sampled. A large value means a busy network. | Number of messages sent to the remote host during the last sampling period (specified using <code>sysinterval</code> ).   |
| GWTDOMAIN     | Number of active outbound requests at the time the data is sampled.  | Number of messages that have been sent to remote domain during the last sampling period (specified using Monitoring Policy Definition <code>sysinterval</code> ). |

## See Also

- [Server Historical Data Query](#)

## Server Historical Data Query

**Server Historical Data Query** page displays Tuxedo server statistical information.

**Note:** Server monitoring data includes both user monitoring data *and* Tuxedo system data.

[Table 1-27](#) list the Server Historical Data Query page properties.

**Table 1-27 Server Historical Data Query Page**

| <b>Name</b>                              | <b>Description</b>   |
|--|--|
| <b>Domain</b>                            | Domain   |
| <b>Machine</b>                           | Machine  |
| <b>Group</b>                             | Group  |
| <b>Server</b>                            | Server   |
| <b>Available Remote Domains or Hosts</b> | 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. |
| <b>Time Interval</b>                     | Time span (minutes)  |
| <b>From</b>                              | Start time (DD MM YYYY HH MM) of time period   |
| <b>To</b>                                | End time (DD MM YYYY HH MM) of time period   |

[Table 1-28](#) lists **Throughput** page properties.

**Table 1-28 Throughput Page**

| <b>Item</b>          | <b>Description</b>   |
|----------------------|--|
| When                 | Time period.   |
| Message Number       | Accumulated number of messages sent by GWTDOMAIN or BRIDGE in the sampling period.             |
| Message Size (bytes) | Accumulated number of the size of messages sent by GWTDOMAIN or BRIDGE 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 a given server during the specified **From** and **To** time range. The X-axis displays the time interval. The Y-axis displays the accumulated number of messages sent to a remote domain or a remote host during the 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. You can:




- specify the partial or complete Global Transaction ID (GTRID) for a specific transaction
- specify the latest time the transaction started
- specify the time period

Clicking **Submit** displays the GTRID general information table. [Table 1-29](#) lists the GTRID general information properties.

**Table 1-29 GTRID General Information Page**

| <b>Name</b>      | <b>Description</b>  |
|------------------|---|
| <b>No.</b>       | Sequence number. Starts at 1.   |
| <b>Initiator</b> | <p>Transaction initiator. Consists of the value of following fields separated by a space:</p> <ul style="list-style-type: none"> <li>a. &lt;DOMAINID&gt;:&lt;master machine name&gt;:&lt;IPCKEY&gt;(see <a href="#">Table 1-12</a>)</li> <li>b. Machine ID (LMID in UBBCONFIG's *MACHINES section)</li> <li>c. Group Name, server only</li> <li>d. Process Name</li> <li>e. Server ID (SRVID in UBBCONFIG's *SERVERS section), server only</li> <li>f. Process ID (pid).</li> </ul> |
| <b>GTRID</b>     | Global Transaction ID.  |

**Table 1-29 GTRID General Information Page**

|                            |  |
|----------------------------|--|
| <p><b>Status</b></p>       | <p></p> <p>Indicates finished request.</p> <p></p> <p>Indicates pending request.</p> <p></p> <p>Indicates failed request.</p> <p><b>Note:</b> The transaction status is determined using the following heuristic rules:</p> <ul style="list-style-type: none"> <li>• The status is displayed as 'failed' if any of the operations has a negative return code.</li> <li>• The status is displayed as 'finished' if:             <ul style="list-style-type: none"> <li>- tpccommit, xa_commit, or tms_xa_commit is called</li> <li>- xa_prepare is called returning XA_RDONLY</li> </ul> </li> <li>• The status is displayed as 'failed' if tpabort, xa_abort, xa_rollback, or tms_xa_rollback is called.</li> </ul> |
| <p><b>Start Time</b></p>   | <p>Transaction start time. The format is 'YY/MM/DD hh:mm:ss:SSS' (SSS = millisecond).</p>  |
| <p><b>Duration</b></p>     | <p>Transaction life time</p>   |
| <p><b>Exec Time</b></p>    | <p>Total time elapsed for all Transaction operations.</p>  |
| <p><b>Parent GTRID</b></p> | <p>The original GTRID for transaction across Tuxedo domain.</p>  |

**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 1-30](#) lists the Transaction Detail page properties.

**Table 1-30 Transaction Detail Information**

| Name              | Description  |
|-------------------|--|
| <b>No.</b>        | Sequence number. Starts at 1.  |
| <b>Location</b>   | where Transaction operation occurred in the same format as “Initiator” in brief table.       |
| <b>XA OP</b>      | Transaction operation name.  |
| <b>Retcode</b>    | Transaction operation return code.   |
| <b>Start Time</b> | Transaction operation start time. The format is ‘YY/MM/DD hh:mm:ss:SSS’ (SSS = millisecond). |
| <b>Exec Time</b>  | 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 the entire GTRID is entered.

**Note:** When **Exact Match** is not checked, all transactions that include a **GTRID** are shown.

2. Click the **Submit** button.
3. Click the **GTRID** to display more information.

## Query Past Transactions

To query past transaction, do the following steps

1. Enter the time interval in **Query for latest** to specify the earliest started transaction; or select time period in **Query during**.
2. Click the **Submit** button.

3. Click a **GTRID** to display more information.

## Get GTRID Call Path Tree information

To get GTRID call information, do the following steps:

1. Enter search information and click the **Submit** 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 for the following reasons:

- a. The call started before the BEA 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 BEA TSAM alerts. It allows you to “**Add**”, “**Edit**” and “**Delete**” BEA TSAM alerts. [Table 1-31](#) lists the Alert Management page properties.

**Table 1-31 Alert Management Page**

| <b>Name</b>        | <b>Description</b>   |
|--------------------|--|
| <b>Name</b>        | Alert name. Must be given when this alert is created.  |
| <b>Type</b>        | Alert type. BEA TSAM supports four alert types: “Call Path”, “Service”, “System” and “Transaction” which correspond to the four performance monitoring categories. |
| <b>Description</b> | Alert description.   |

**Table 1-31 Alert Management Page**

|               |                          |
|---------------|--------------------------|
| <b>Add</b>    | Add a new alert          |
| <b>Edit</b>   | Edit a selected alert    |
| <b>Delete</b> | 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 1-32](#) lists the Alert Definition page properties.

**Table 1-32 Alert Definition Page**

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

**Table 1-32 Alert Definition Page**

|                                |   |
|--------------------------------|---|
| <p><b>Alert Definition</b></p> | <p>Defines the items that generate an event. They are alert-type specific.</p> <p><b>Call Path Type:</b></p> <ul style="list-style-type: none"> <li>• <b>Elapse time.</b><br/>The time elapsed since this request was monitored. An event is generated once the time threshold is reached. The unit is in milliseconds.</li> <li>• <b>IPC Queue Length.</b><br/>The request IPC queue length on the call path tree of the monitored request. It is an integer threshold that generates an event if any request queue length exceeds the defined value.</li> <li>• <b>Execution Error.</b><br/>Boolean threshold that generates events when Tuxedo service execution encounters error.</li> </ul> <p><b>Service Type</b></p> <ul style="list-style-type: none"> <li>• <b>Execution time.</b><br/>The elapsed execution time for a service. An event is generated once the time threshold is reached. The unit is in milliseconds.</li> <li>• <b>IPC Queue Length.</b><br/>The monitored application server request IPC queue length. It is an integer threshold that generates events if the queue length exceeds the defined value.</li> <li>• <b>Execution Error.</b><br/>Boolean threshold that generates events when Tuxedo service execution encounters error.</li> <li>• <b>Waiting Time in Queue.</b><br/>Numeric threshold that generates events when the waiting time in the IPC queue goes beyond the defined value. The unit is in milliseconds.</li> </ul> |
|--------------------------------|---|

Table 1-32 Alert Definition Page

|                    |  |
|--------------------|--|
|                    | <p><b>System Type</b></p> <ul style="list-style-type: none"> <li>• <b>Network Link Lost.</b><br/>An event is generated when a network link is lost. If the link is not connected, the event is generated periodically by the monitoring interval.</li> </ul> <p><b>Transaction Type</b></p> <ul style="list-style-type: none"> <li>• <b>Transaction Call Failure.</b><br/>The XA call failure results in event generation based on Transaction Call Failure criteria. For example, if an <code>xa_commit()</code> return code is less than 0, a Transaction Call Failure event is generated."</li> </ul> |
| <b>Severity</b>    | <p>Four security levels can be selected:</p> <ul style="list-style-type: none"> <li>• <b>Information</b></li> <li>• <b>Warn</b></li> <li>• <b>Critical</b></li> <li>• <b>Fatal</b></li> </ul>  |
| <b>Action</b>      | <p>The action defines which action need to be performed when the evaluation is true. Current only <b>Tuxedo Event</b> is supported. When <b>Tuxedo Event</b> is selected, <b>Tuxedo Event Name</b> and <b>Tuxedo Event Message</b> must be supplied.</p>   |
| <b>Description</b> | <p>A description string for this alert</p>   |

## See Also

- [Event Query](#)

## Events

The **Events** page displays current BEA TSAM-generated events. The **Show All Events** button lists all the events.

Click the **Show Filter** button; the **Filter Conditions** panel appears. After the **Show Filter** button is clicked, it changes to the **Hide Filter** button. Click the **Hide Filter** button; the **Filter Conditions** panel is hidden.

Click the **Submit** button in the **Filter Conditions** panel to list events based on the filter criteria.

**Table 1-33 Events Page**

| <b>Name</b>                    | <b>Description</b>  |
|--------------------------------|---|
| <b>Show All Events</b>         | Lists all events in detail  |
| <b>Show/Hide Filter</b>        | Show/Hide <b>Filter Conditions</b> panel  |
| <b>Delete Events</b>           | Delete selected events.<br><b>Note:</b> The <b>Delete Events</b> button appears only if events are available in the database. |
| <b>Delete All Events</b>       | Delete all events in database.<br><b>Note:</b> same as <b>Delete Events</b> .   |
| <b>Show XX Events per Page</b> | Displays the selected number of events per page.  |

**Table 1-34 Filter Conditions Panel**

| <b>Name</b>       | <b>Description</b>   |
|-------------------|--|
| <b>Event Name</b> | Event name. Lists available alerts. “Any” indicates all events are searched.                     |
| <b>Catalog</b>    | Lists Catalog Type: <ul style="list-style-type: none"> <li>● Alert</li> <li>● Plug-in</li> </ul> |

**Table 1-34 Filter Conditions Panel**

| <b>Name</b>              | <b>Description</b>   |
|--------------------------|--|
| <b>Event Type</b>        | Lists event type: <ul style="list-style-type: none"> <li>• Call Path</li> <li>• Service</li> <li>• System</li> <li>• Transaction</li> </ul>  |
| <b>Event Severity</b>    | Lists event severity: <ul style="list-style-type: none"> <li>• Information</li> <li>• Warning</li> <li>• Critical</li> <li>• Fatal</li> </ul> <p><b>Note:</b> Information is lowest. Fatal is highest.</p> |
| <b>Include and below</b> | If checked, all events with the selected Event Severity and higher Severity are listed.<br>If unchecked, only the events under a particular Event Severity are included.                                   |
| <b>From</b>              | Start time (DD MM YYYY HH MM)  |
| <b>To</b>                | End time (DD MM YYYY HH MM)  |
| <b>Submit</b>            | Lists all event details based on the filter condition  |

[Table 1-35](#) lists the Event Details page properties.

**Table 1-35 Events Detail Page**

| <b>Name</b>        | <b>Description</b>   |
|--------------------|--|
| <b>Report Time</b> | Timestamp when an event is reported  |
| <b>Location</b>    | The location where the metrics are evaluated that generate a current event. It has the same format as Call Path Tree.  |
| <b>Catalog</b>     | <p>The event generation source. Currently, BEA TSAM supports two sources:</p> <ul style="list-style-type: none"> <li>• Alerts defined in the BEA TSAM console,</li> <li>• Plug-in events directly generated by the BEA TSAM Agent.</li> </ul> <p>For more information, see BEA TSAM Agent in the <i>Tuxedo System and Application Monitor (BEA TSAM) Administration Guide</i>.</p> |
| <b>Name</b>        | The event name. For alert events, it is the name of the alert. For plug-in events, it is the name defined in event trigger configuration file  |
| <b>Type</b>        | <p>Event type corresponding to the four monitoring types:</p> <ul style="list-style-type: none"> <li>• call path</li> <li>• service</li> <li>• system</li> <li>• transaction</li> </ul> <p>Plug-in events can only be generated for call path and service.</p>   |
| <b>Severity</b>    | <p>Event severity specified in the alert definition page or event trigger configuration file. Four severity levels are supported:</p> <ul style="list-style-type: none"> <li>• Information</li> <li>• Warn</li> <li>• Critical</li> <li>• Fatal</li> </ul>   |



**Table 1-35 Events Detail Page**

| Name               | Description  |
|--------------------|--|
| <b>Description</b> | <p>The event description It depends on the event type, source and conditions.</p> <p>For alert-generated events, the descriptions are:</p> <p><b>Call Path Monitoring:</b></p> <ul style="list-style-type: none"> <li data-bbox="417 539 1032 656">• Elapsed Time<br/>Format: “Application (call path correlation ID) elapsed time exceeded limit [defined limit:measured value] CORRID (correlation ID)”.</li> <li data-bbox="417 673 1079 760">• IPC Queue Length<br/>Format: “Service (service name) IPC queue length exceeded limit [defined limit:measured value] CORRID (correlation ID)”</li> <li data-bbox="417 777 1069 864">• Execution Error<br/>Format: “Service (service name) execution failed. Tuxedo errno number xxx CORRID (correlation ID)”</li> </ul> <p><b>Service Monitoring:</b></p> <ul style="list-style-type: none"> <li data-bbox="417 921 1063 1008">• Execution Time.<br/>Format: “Service (service name) execution time exceeded limit [defined limit:measured value] SVCNAME (service name)”</li> <li data-bbox="417 1025 1079 1112">• IPC Queue Length.<br/>Format: “Service (service name) IPC queue length exceeded limit [defined limit:measured value] SVCNAME (service name)”</li> <li data-bbox="417 1130 1069 1216">• Execution Error.<br/>Format: “Service (service name) execution failed. Tuxedo errno number xxx SVCNAME (service name)”</li> <li data-bbox="417 1234 1022 1350">• Waiting Time in Queue.<br/>Format: “Service (service name) IPC queue waiting time exceeded limit [defined limit:measured value] SVCNAME (service name)”</li> </ul> |

**Table 1-35 Events Detail Page**

| Name | Description   |
|------|---|
|      | <p><b>System Monitoring:</b></p> <ul style="list-style-type: none"> <li>• Network Link Lost:           <ul style="list-style-type: none"> <li>– GWTDOMAIN<br/>Format: “Remote domain xxx connection lost”. “xxx” is the remote domain name defined in DMCONFIG.</li> <li>– BRIDGE<br/>Format: “Remote machine xxx connection lost”. “xxx” is the remote machine name.</li> </ul> </li> </ul> <p><b>Transaction Monitoring:</b></p> <ul style="list-style-type: none"> <li>• Transaction Call Failure.<br/>Format: “XA routine (routine name) execution failed. Error number xxx GTRID (xxx)”</li> </ul> <p>For plug-in generated events, the descriptions are:</p> <p><b>Call Path Monitoring:</b></p> <ul style="list-style-type: none"> <li>• Format:<br/>Plug-in generated event CORRID (Correlation ID) SVCNAME (service name) DEPTH (depth on call path tree) ERRNO (Tuxedo error number) URCODE (tpretreturn user return code)</li> </ul> <p><b>Service Monitoring:</b></p> <ul style="list-style-type: none"> <li>• Format:<br/>Plug-in generated event SVCNAME (service name) URCODE (tpretreturn user return code of) EXEETIME (service execution time) MSGQUEUED (message queued on the request IPC queue)</li> </ul> |

## Show All Events

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

## Filter Events

To filter events, do the following steps:

1. Click the **Show Filter** button; the **Filter Conditions** panel appears.
2. Select the **Event Name, Catalog, Event Type, Event Severity**, and time period (**From, To**).

3. Click the **Submit** button; the events matching the **Filter Conditions** panel are listed.
4. Click the **Hide Filter** button to hide the **Filter Conditions** panel.

**Note:** If you want to display the exact event severity, uncheck the **Include and below** check box.

## Delete Events

To delete events, do the following steps:

1. Click the check box next to the event you want to delete.

You can also click the check box in the header row to select all events on the current page.

2. Click the **Delete Events** button to delete selected events. An event summary is displayed at the bottom of the table.

## Delete All Events

Clicking the **Delete All Events** button removes all the events stored in the database.

## See Also

- [Alert Management](#)

## Recent Events

The bottom-left panel of the BEA TSAM console lists a summary of generated events. Clicking the event Severity in the panel lists the events on the **Recent Events** page. The event details page layout is similar to the **Alerts/Events** page.

**Note:** Recent Events only include Events that were generated during the last **Event Cache Time**.

## Clean the Event in Cache

Clicking the **Clean** button clears all the events stored in cache. Events can also be queried on the **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 BEA TSAM `web.xml` file. The default value is 60 minutes.

## See Also

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

